

"Vraagmaatje, wat gebeurt er met mijn persoonsgegevens?"

*Een praktijkgericht juridisch onderzoek naar de wijze waarop VM-Concepts
de gewenste verwerking van persoonsgegevens dient in te richten,
zodat deze voldoet aan de Algemene verordening gegevensbescherming*



Bron foto: Lumipeople.com

Mick van Assen
Juridische Hogeschool Avans-Fontys

VM-Concepts
Tilburg, mei 2017

Vr@@g MAATJE

Juridische Hogeschool
Avans-Fontys

”Vraagmaatje, wat gebeurt er met mijn persoonsgegevens?”

*Een praktijkgericht juridisch onderzoek naar de wijze waarop VM-Concepts de
gewenste verwerking van persoonsgegevens dient in te richten, zodat deze voldoet
aan de Algemene verordening gegevensbescherming*

Auteur:	Mick van Assen
Studentnummer:	2071816
Onderwijsinstelling:	Juridische Hogeschool Avans-Fontys
In opdracht van:	VM-Concepts
Afstudeerperiode:	6 februari 2017 t/m 28 mei 2017
Afstudeermentor:	mr. D.P.M.G. van den Boom
Eerste afstudeerdocent:	mr. T.C.F.M. Vermeulen
Tweede afstudeerdocent:	mr. N. Deters-Vermijs
Classificatie:	Intern

Disclaimer: de informatie in dit rapport, inclusief bijlagen, is vertrouwelijk en uitsluitend bestemd voor de geadresseerde. Verstrekking aan en gebruik door anderen dan de geadresseerde is zonder toestemming niet toegestaan.

Voorwoord

Vol trots presenteer ik dit onderzoeksrapport, tevens dienende als mijn afstudeerscriptie, met de titel "Vraagmaatje, wat gebeurt er met mijn persoonsgegevens?". Deze titel verwoordt het onderwerp vanuit het perspectief van een gebruiker van Vraagmaatje. Deze maakt gebruik van Vraagmaatje door een vraag te stellen en vraagt zich tegelijkertijd af wat er vervolgens met zijn persoonsgegevens gebeurt.

Dit onderzoeksrapport is opgesteld in opdracht van VM-Concepts. Ik bedank de personen achter deze organisatie dan ook, te weten: Ronald Meulendijks, Frank van Rooy en in het bijzonder Nico van den Boom. Nico van den Boom was tevens mijn stagebegeleider en heeft mij ondersteund op de momenten dat het nodig was. Ook heeft hij zijn kennis van en zicht op het recht op een fijne manier gedeeld. Daarnaast heb ik in de periode van 6 februari t/m 28 mei een interessante stage mogen meemaken bij zijn organisatie Boom Advocatenkantoor, gelieerd aan Advocabo. Ronald Meulendijks en Frank van Rooy dank ik voor het feit dat zij altijd bereid waren om mijn vragen over VM-Concepts te beantwoorden.

Bovendien bedank ik Edith Mostert en Marieke Pette van KBO-Brabant voor hun medewerking, waaronder voor het in contact brengen met de KBO-leden en de verspreiding van mijn enquête.

Verder gaat mijn dank uit naar de Juridische Hogeschool Avans-Fontys door mij in de gelegenheid te stellen mijn studie aan haar instelling te laten volgen. Zo ook in deze laatste fase van mijn studie, met behulp van mijn afstudeerdocenten Thom Vermeulen en Noor Deters-Vermijs. Thom Vermeulen verdient als vast aanspreekpunt en goede begeleider een bijzonder dankwoord. Zijn deskundigheid, oplossingsgerichtheid en flexibiliteit hebben er mede voor gezorgd dat ik trots mag zijn op de oplevering van dit rapport.

Ten slotte bedank ik mijn vriendin voor haar onvoorwaardelijke steun en toeverlaat, zowel tijdens het schrijven van dit rapport als tijdens de rest van mijn studie.

Na een interessante studie van vier jaar is het een eer om met dit onderzoeksrapport mijn studie af te mogen sluiten. Ik wens u dan ook veel leesplezier.

Mick van Assen

Tilburg, mei 2017

Inhoudsopgave

Samenvatting

Afkortingenlijst

Begrippenlijst AVG

1. Inleiding	9
§ 1.1 Organisatiebeschrijving	9
§ 1.2 Probleembeschrijving	9
§ 1.3 Centrale vraag en deelvragen	10
§ 1.4 Doelstelling	11
§ 1.5 Onderzoeksmethodiek en verantwoording	11
§ 1.6 Leeswijzer	12
2. Privacy en gegevensbescherming	13
§ 2.1 Historie van vanuit drie perspectieven	13
§ 2.1.1 Nationaal perspectief	13
§ 2.1.2 Internationaal perspectief	14
§ 2.1.3 Europees perspectief	14
§ 2.2 Totstandkoming Wbp en AVG	14
§ 2.3 Belangrijkste verschillen Wbp en AVG	15
§ 2.4 Huidige en toekomstige gegevensverwerking: Big Data	16
3. Algemene verordening gegevensbescherming	17
§ 3.1 Reikwijdte AVG	17
§ 3.1.1 Natuurlijke personen	17
§ 3.1.2 Materieel en territoriaal toepassingsgebied	17
§ 3.1.3 Persoonsgegevens	18
§ 3.1.4 Verwerking	19
§ 3.2 Beginselen voor verwerking	20
§ 3.3 Bijzondere verwerking	24
§ 3.4 Rechten betrokkenen	25
§ 3.5 Verantwoordelijkheden wvv en verwerker	29
§ 3.6 Persoonsgegevensbeveiliging	30
§ 3.7 Privacy Impact Assessment en voorafgaande raadpleging	32
§ 3.7.1 Privacy Impact Assessment (PIA)	32
§ 3.7.2 Voorafgaande raadpleging	32
§ 3.8 Functionaris voor gegevensbescherming	33
§ 3.9 Autoriteit Persoonsgegevens en sanctiebevoegdheid	33
§ 3.9.1 Taken en bevoegdheden	33
§ 3.9.2 Sanctiebevoegdheid	34
4. Praktijksituatie VM-Concepts	35
§ 4.1 VM-Concepts	35
§ 4.2 Vraagmaatje	35
§ 4.3 Financiële aspecten	36
§ 4.4 Verwerking van persoonsgegevens	37
§ 4.5 Voorgenomen beveiliging	38
§ 4.6 Ethische aspecten	38

5. Conclusies en aanbevelingen	39
§ 5.1 Conclusies	39
§ 5.2 Aanbevelingen	44

Bronnenlijst

Bijlagen

Bijlage I	Uitwerking interview met de heer Van den Boom
Bijlage II	Uitwerking interview met de heer Meulendijks
Bijlage III	Uitwerking interview met de heer Van Rooy
Bijlage IV	Enquête gegevensgebruik Vraagmaatje

Samenvatting

Een aantal initiatiefnemers zijn een startup begonnen genaamd “VM-Concepts”, met het plan om een digitale omgeving te creëren met de naam “Vraagmaatje”. VM-Concepts (VMC) is opgericht als bv met een ‘social enterprise-principe’. Dit betekent dat geld verdienen niet het hoofddoel is, maar geld wel een middel is om bij te kunnen dragen aan de maatschappij. VMC wil bijdragen door het leveren van een dienst in de vorm van Vraagmaatje. Het is de bedoeling dat Vraagmaatje dient als een digitale vraagbaak; een digitale buddy, met name voor ouderen. In deze digitale omgeving zullen zich namelijk allerlei applicaties bevinden waar een Vraagmaatje-gebruiker beroep op kan doen. Deze toepassingen hebben tot gezamenlijk doel het ondersteunen van gebruikers bij zo veel mogelijk formele zaken die door gebruikers als complex kunnen worden ervaren.

Een van de applicaties is een persoonlijke mailbox voor de gebruiker. Het zal voor de gebruiker mogelijk zijn om in deze ‘digitale brievenbus’ e-mails en relevante stukken van allerlei organisaties te ontvangen. Een andere applicatie binnen Vraagmaatje zal deze analyseren en beoordelen, en de gebruiker adviseren over welke actie door hem moet worden ondernomen. Achter Vraagmaatje zal menselijke ondersteuning aanwezig zijn voor als Vraagmaatje een gebruiker niet juist of niet tijdig kan ondersteunen. VMC wil Vraagmaatje tegelijkertijd autodidact maken, zodat Vraagmaatje uiteindelijk de meeste handelingen zelfstandig kan uitvoeren en de gebruiker steeds beter en sneller kan worden geholpen met zijn vraagstukken.

Al met al brengt dit veel verwerkingen van persoonsgegevens met zich mee, waardoor VMC verplicht is om aan de Algemene verordening gegevensbescherming (AVG) te voldoen. In dit onderzoeksrapport worden die verplichtingen getoetst aan de gewenste werkwijze van VMC en wordt aangegeven hoe VMC deze verplichtingen in dient te richten. Een organisatie die onder de reikwijdte van de VMC valt zal in ieder geval de beginselen voor gegevensverwerking moeten naleven. Belangrijke beginselen hierbij zijn het transparantie- en rechtmatigheidsbeginsel. Een bedrijf dat een dienst levert zal de rechtmatigheidsgrond voor de verwerking moeten baseren op de uitdrukkelijke toestemming van de betrokkene. Daarnaast moet een dergelijke organisatie te allen tijde de rechten van betrokkenen in acht te nemen, zoals het recht op inzage of gegevenswissing. Bovendien kan een organisatie te maken krijgen met pseudonimisering en anonimisering, bijvoorbeeld wanneer zij van persoonsgegevens metadata wil vormen.

Ook is er de kans dat er een datalek plaatsvindt met als mogelijk gevolg dat de rechten van een betrokkene risico lopen. Onder bepaalde voorwaarden is er dan een meldingsplicht aan de betrokkene en/of aan de Autoriteit Persoonsgegevens. Verder dient er in sommige gevallen een functionaris voor gegevensbescherming te worden aangesteld en kan de organisatie verplicht worden voorafgaand aan een verwerking een Privacy Impact Assessment (PIA) uit te voeren. Indien de PIA aangeeft dat er een hoog risico voor de betrokkene is, is een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens vereist.

Voorafgaand aan het aanbieden van een dienst waar de verwerking van persoonsgegevens relevant bij is, dienen ook een aantal maatregelen genomen te worden. Zo moet zij zowel haar verantwoordelijkheden als de doeleinden voor de verwerking vaststellen. Daarnaast dient een organisatie gegevensbeschermingsbeleid opstellen met daarin een uitleg aan de betrokkene over welke persoonsgegevens met welke doeleinden worden verwerkt.

Afkortingenlijst

Afkorting	Betekenis
AP	Autoriteit Persoonsgegevens (voormalig: CBP)
art.	artikel
AVG	Algemene verordening gegevensbescherming (ook wel: "Privacyverordening")
BW	Burgerlijk Wetboek
CBS	Centraal Bureau voor de Statistiek
CBP	College bescherming persoonsgegevens
EU	Europese Unie
e.v.	en volgende
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
FG	Functionaris voor de gegevensbescherming
Gw	Grondwet
i.o.	in oprichting
IVBPR	Internationaal Verdrag inzake burgerrechten en politieke rechten
jo.	juncto
MvT	Memorie van Toelichting
overw.	overweging(motivering (hier: in de Preamble) van de inhoud van een artikel, begrip of beginsel)
PIA	Privacy Impact Assessment
Privacyrichtlijn	Richtlijn (95/46/EG) van het Europese Parlement en de Raad van 24 oktober 1995
Preamble	Preamble van de Privacyverordening
Privacyverordening	Verordening (EU) 2016/679 van het Europees Parlement en de Raad, van 27 april 2016 (AVG)
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
VvS	Verdrag van Straatsburg
VwEU	Verdrag betreffende de werking van de Europese Unie
Vwv	Verwerkingsverantwoordelijke
Wabb	Wet algemene bepalingen burgerservicenummer
Wbp	Wet bescherming persoonsgegevens
Wmd	Wet meldplicht datalekken
Wpr	Wet persoonsregistraties

Begrippenlijst AVG (onder andere op basis van art. 4)

Begrip	Betekenis
Autoriteit Persoonsgegevens (AP)	Bevoegd toezichthoudend bestuursorgaan voor het toezicht op de verwerking van persoonsgegevens in Nederland (voorheen: CBP)
Bestand	Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid
Betrokkene	Een geïdentificeerde of identificeerbare natuurlijke persoon waarvan de persoonsgegevens worden verwerkt
Biometrische gegevens	Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens
Derde	Een natuurlijke persoon of rechtspersoon, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken
Genetische gegevens	Persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon
Ontvanger	Een natuurlijke persoon of rechtspersoon, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt
Overweging	Motivering (hier: in de preambule van de AVG) van de inhoud van een artikel, begrip of beginsel
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon
Profilering	Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen
Pseudonimisering	Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er

	aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld
Verwerker	Een natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (voorheen: bewerker). Dit is vrijwel altijd een instelling of persoon die zich buiten de organisatie van de verwerkingsverantwoordelijke bevindt en die niet in hiërarchische relatie tot hem staat ¹
Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens
Verwerkingsverantwoordelijke	Een natuurlijke persoon of rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (voorheen: verantwoordelijke). Dit is in de private sector de natuurlijke persoon of rechtspersoon onder wiens verantwoordelijkheid de gegevensverwerking plaatsvindt. ² Dit begrip zal in dit rapport gemakshalve worden afgekort als 'vvv'.

¹ Kamerstukken II 1997/98, 25892, 3, p. 61.

² Kranenborg & Verhey 2011, p. 76 en Kamerstukken II 1997/98, 25892, 3, p. 55.

Hoofdstuk 1 Inleiding

§ 1.1 Organisatiebeschrijving

Advocabo is sinds 2014 een innovatieve startup in de juridische dienstverlening. Zij heeft als doel het verbinden van rechtzoekenden met advocaten met bewezen kwaliteit. Als een cliënt zich met een juridisch probleem tot Advocabo richt, zoekt Advocabo naar de meest geschikte advocaat binnen haar netwerk van aangesloten advocaten. Zo wordt voorkomen dat een advocaat die niet in het betreffende rechtsgebied gespecialiseerd is, de zaak van een cliënt toch aanneemt en wordt ervoor gezorgd dat een cliënt de best beschikbare hulp toekomt. Het motto van Advocabo is dan ook: *'creating a better legal future'*. Advocabo wordt geleid door de heer mr. D.P.M.G. (Nico) van den Boom.

§ 1.2 Probleembeschrijving

In december 2016 richtten een drietal initiatiefnemers, te weten de heer Van den Boom, de heer Meulendijks en de heer Van Rooy, zich tot het Avans Ondernemerscentrum (hierna: AOC) met een vraagstuk. Het AOC is een loket voor bedrijven en instellingen dat onderzoekers, docenten en studenten samen laat werken aan multidisciplinaire vraagstukken.³ Het voornoemde vraagstuk staat in het kader van de oprichting van een startup, welke 'VM-Concepts' zal heten (hierna ook wel: VMC). De initiatiefnemers bekijken op dit moment namelijk de mogelijkheden om een samenwerking aan te gaan met elkaar en met een aantal partners, met als doel het inzetten van technologie om burgers te helpen met allerlei zaken die zij als complex kunnen ervaren. Dit wil zij doen door het creëren van een platform genaamd 'Vraagmaatje'.

Vraagmaatje zal fungeren als een portaal⁴ waarbinnen allerlei applicaties die werken met nieuwe technologieën toegankelijk worden gemaakt voor gebruikers van Vraagmaatje. Deze toepassingen hebben verschillende functies, maar hetzelfde doel: de gebruiker van Vraagmaatje ontzorgen door deze te ondersteunen bij allerlei formele zaken en zo tegelijkertijd (potentieel juridische) conflicten vroegtijdig te voorkomen. Dit doen de applicaties voornamelijk door de gebruiker te adviseren over deze formele kwesties. Een belangrijke toepassing hiervoor is een persoonlijke mailbox waar de gebruiker mails en relevante stukken binnenkrijgt van verschillende organisaties. Hierbij kan worden gedacht aan beschikkingen van gemeenten en betaalspecificaties of telefoonabonnementen van leveranciers van telecommunicatie. Een belangrijke doelgroep voor Vraagmaatje zijn de leden van de belangenbehartigingsorganisatie voor senioren: 'KBO-Brabant'⁵.

Voor dit vraagstuk heeft het AOC aan drie studenten commerciële economie gevraagd een marktonderzoek te verrichten en aan mij als rechtenstudent gevraagd een onderzoeksrapport op te stellen. Hierbij zal regelmatig worden samengewerkt, waardoor dit onderzoek tevens een multidisciplinaire opdracht is. In het marktonderzoek wordt bekeken welke reeds bestaande applicaties kunnen worden betrokken bij Vraagmaatje. Hierdoor worden de beschikbare technieken van deze applicaties in Vraagmaatje betrokken en waar mogelijk toegankelijk gemaakt.

De juridische aspecten die VMC getoetst wil hebben, staan in het teken van privacyrecht, om specifiek te zijn het recht op gegevensbescherming. VMC is namelijk voornemens om bij het gebruik van Vraagmaatje door een gebruiker veel (soorten) persoonsgegevens te verwerken. Het gaat hierbij zowel om 'directe' persoonsgegevens, zoals naam, adres en geboortedatum, als om alle relevante gegevens over de formele zaken waar betrokkenen ondersteuning bij vragen. Bij formele zaken dient te worden gedacht aan onderwerpen als financiën,

³ Het Avans Ondernemerscentrum, Avans.nl.

⁴ Een poortal (portal) is een online omgeving die toegang geeft tot verschillende websites of applicaties.

⁵ KBO-Brabant; Kbo-brabant.nl.

gezondheid, zorg en administratie. Met al deze gegevens wil VMC een aantal doelen nastreven:

- potentiële (juridische) problemen voorkomen door vroegtijdige herkenning en oplossing daarvan;
- database Vraagmaatje uitbreiden en deze op autodidacte wijze beter laten functioneren, waardoor steeds meer gebruikers optimaal kunnen worden geholpen;
- informatie (metadata) verstrekken aan contractspartijen, zoals gemeenten, politie, overheidsinstellingen en bedrijven die daarmee hun werkwijzen en klantenservices kunnen verbeteren.

Deze verwerkingen van persoonsgegevens worden in dit rapport getoetst aan de Algemene verordening gegevensbescherming (AVG) die op 25 mei 2016 in werking is getreden.⁶ Ondanks deze inwerkingtreding hebben organisaties tot 28 mei 2018 de tijd om hun werkwijzen hieraan aan te passen. Deze Europese privacyverordening vervangt de huidige nationale privacywetgeving van alle EU-landen. Voor Nederland betekent dit concreet dat de Wet bescherming persoonsgegevens (Wbp) zal komen te vervallen. De bepalingen uit de AVG moeten nog wel uitvoering krijgen in de lidstaten. In Nederland is met het oog daarop inmiddels een conceptversie van de Uitvoeringswet van de AVG (UAVG) gepubliceerd.⁷

De toetsing van de voornoemde verwerkingen van persoonsgegevens aan de AVG brengt een aantal vraagstukken met zich mee. Onder welke voorwaarden mogen persoonsgegevens worden verzameld en aan elkaar gekoppeld? En hoe moeten de rechten van gebruikers van Vraagmaatje worden gewaarborgd? Een ander relevant vraagstuk in dit kader is in hoeverre gebruikers van Vraagmaatje zouden kunnen betalen met gegevens in plaats van met geld.

§ 1.3 Centrale vraag en deelvragen

De vraag die volgt uit de probleembeschrijving en tevens centraal staat in dit onderzoeksrapport luidt als volgt: “op welke wijze dient VM-Concepts de gewenste verwerking van persoonsgegevens in te richten, zodat deze voldoet aan de Algemene verordening gegevensbescherming?”.

Ter beantwoording van de centrale vraag kan deze worden onderverdeeld in een aantal deelvragen:

- Welke eisen stelt de Algemene verordening gegevensbescherming aan de verwerking van persoonsgegevens?
- In hoeverre worden deze eisen nader uitgelegd en aangevuld door de Wet bescherming persoonsgegevens en de daarbij aanverwante jurisprudentie en memorie van toelichting?
- In hoeverre worden deze eisen nader uitgewerkt en gespecificeerd in de conceptversie Uitvoeringswet Algemene verordening gegevensbescherming?
- Op welke wijze worden VMC en het platform Vraagmaatje opgericht en ingericht?
- Wat is de gewenste werkwijze van VMC met betrekking tot Vraagmaatje en persoonsgegevensverwerking?

⁶ Verordening (EU) 2016/679.

⁷ Uitvoeringswet Algemene Verordening Gegevensbescherming. Te bereiken via Internetconsultatie op Overheid.nl.

§ 1.4 Doelstelling

Het doel van dit onderzoek is om op 28 mei 2017 bij de initiatiefnemers van VMC een rapport af te leveren, waarin aan de hand van een beschrijving van de praktijk en het recht een oordeel wordt gegeven over de vraag op welke wijze VM-Concepts de gewenste verwerking van persoonsgegevens dient in te richten, zodat deze voldoet aan de Algemene verordening gegevensbescherming en zij op basis van dit oordeel duidelijke handvatten krijgt in de vorm van een checklist en stroomdiagram die zij kan toepassen op haar werkwijzen, waardoor de privacy van gebruikers van Vraagmaatje wordt gewaarborgd.

§ 1.5 Onderzoeksmethodiek en verantwoording

Om te zorgen voor een compleet, onderbouwd en controleerbaar antwoord op de deelvragen en uiteindelijk de centrale vraag, moeten de relevante onderzoeksstrategieën, bronnen en methoden concreet worden vastgesteld en verantwoord. Al het bovenstaande draagt bij aan een systematisch, geobjectiveerd onderzoek naar een antwoord op de centrale vraag

Voor de beantwoording van deelvragen 1 en 2 is het recht onderzocht door rechtsbronnen- en literatuuronderzoek. Hierbij zijn inhoudsanalyses gedaan van relevante rechtsbronnen, literatuur en documenten. De voornaamste rechtsbronnen die zijn bestudeerd zijn de wettekst van de AVG, de conceptwettekst van de Uitvoeringswet AVG (UAVG) en de Wbp, alsmede de beschikbare, aanverwante jurisprudentie. Jurisprudentie zorgt voor een verruimende uitleg van een rechtsregel en zal binnen dit onderzoek worden gebruikt als aanvulling op rechtsregels uit de AVG. Ondanks het feit dat de Wbp nog van kracht is en de AVG nog in de implementatiefase zit, is toch gefocust op de AVG. De reden hiervoor is dat het gaat om een voorgenomen startup en de overgang van de Wbp naar de AVG op relatief korte termijn plaatsvindt. Dit is tevens de wens van VM-Concepts. De Wbp is wel geraadpleegd voor onderwerpen en begrippen die ten opzichte van de AVG (vrijwel) onveranderd zijn. Bovendien komen in dit rapport een aantal juridische onderwerpen aan bod die raakvlakken hebben met onderwerpen uit de AVG, zonder dat deze uitgebreid worden behandeld vanwege de afbakening van dit onderzoek. Voorbeelden hiervan zijn de leerstukken wilsovereenstemming, wilsgebreken en algemene voorwaarden.

Verder wordt literatuuronderzoek verricht naar naslagwerken betreffende privacy en gegevensbescherming. Daarbij wordt alleen gebruikgemaakt van door vakgeleerden erkende literatuur. Deze literatuur zorgt voor aanvullende kennis over voornoemde onderwerpen. In de literatuurlijst van het onderzoeksrapport wordt alle gebruikte literatuur opgesomd. Voor het documentenonderzoek worden publicaties zoals rapporten, uittreksels en artikelen van deskundige, erkende organisaties zoals de Autoriteit Persoonsgegevens en de Europese Commissie gebruikt. Bij internetbronnen is de kwaliteit getoetst met behulp van een checklist die is samengesteld door H.S.M. Driessen, docente aan de Juridische Hogeschool Avans-Fontys. Deze checklist is overgelegd aan de betrokken afstudeerdocent en –mentor.

Ook is overheidsinformatie geraadpleegd, te weten de memorie van toelichting (MvT) op de Wbp (Kamerstuk) en Internetconsultatie in de vorm van de totstandkomingsgeschiedenis van de AVG. Hieronder valt onder andere de conceptversie van de MvT op de Uitvoeringswet AVG (UAVG). Door deze bronnen te analyseren kunnen wetsartikelen in een bredere context worden gezien en zo, vanuit het oogpunt van de wetgever, beter begrepen worden. Hierbij is te allen tijde eerst de totstandkomingsgeschiedenis van de AVG geraadpleegd, alvorens de MvT op de Wbp is bestudeerd. Er wordt in het juridische kader dan ook regelmatig naar deze MvT verwezen, omdat andere bronnen te beperkt zijn. Ondanks deze wellicht ongebruikelijke wijze, is hiervoor gekozen om zo een duidelijker beeld te krijgen van bepaalde onderwerpen en begrippen die materieel niet of nauwelijks zijn gewijzigd ten opzichte van de Wbp.

Deelvragen 3 en 4 zijn praktijkgericht en behoeven daarom kwalitatieve, praktijkgerichte onderzoeksstrategieën. Er is een grondige casestudy verricht door bestudering van het onderwerp persoonsgegevens en de bescherming daarvan, in relatie tot VMC. Bovendien

heeft er een kwalitatief survey-onderzoek plaatsgevonden naar de meningen van vijftien leden van KBO-Brabant. Hierbij is vanuit de juridische aspecten gefocust op de vraag wat deze respondenten vinden van het gebruik van zijn persoonsgegevens door VMC.

Bij deze casestudy en survey zijn meerdere onderzoeksmethoden gecombineerd. Allereerst zijn bij de casestudy de meest betrokken, relevante personen geïnterviewd, te weten de initiatiefnemers van Vraagmaatje: de heer Van den Boom, de heer Meulendijks en de heer Van Rooy. Deze personen staan het dichtst bij de praktijksituatie, waardoor deze voor het nagaan hiervan het meest betrouwbaar zijn. Tijdens deze interviews zijn op een objectieve en waar nodig kritische manier open vragen gesteld. Na de interviews zijn deze nagestuurd naar de betreffende persoon met de vraag deze te autoriseren. Daarnaast zijn inhoudsanalyses gemaakt van relevante, praktijkgerichte documenten, zoals van PowerPointpresentaties die door de initiatiefnemers van VMC zijn gemaakt. Bij de survey is gebruikgemaakt van een objectieve vragenlijst met specifieke, begrijpelijke vragen. Hierbij is besloten om de enquête te richten tot tien leden van KBO-Brabant die al eerder betrokken zijn geweest bij vergaderingen en workshops over Vraagmaatje. Dit zijn potentiële gebruikers die voorkennis hebben van (de plannen met betrekking tot) Vraagmaatje en zijn derhalve de meest geschikte respondenten voor deelneming aan de enquête.

§ 1.6 Leeswijzer

In het eerstvolgende hoofdstuk zal eerst worden stilgestaan bij de ontwikkeling van privacyrecht en gegevensbescherming. Hierbij zal tevens worden toegelicht hoe de Wbp en AVG tot stand zijn gekomen en wat de belangrijkste veranderingen zijn met de inwerkingtreding van de AVG. Vervolgens wordt in hoofdstuk 3 het juridisch kader uitgediept en wordt zo een basis gevormd voor de beantwoording van deelvraag 1 t/m 3. In hoofdstuk 4 wordt de praktijksituatie aangaande VMC en Vraagmaatje in kaart gebracht, wat bijdraagt aan de beantwoording van deelvraag 4 en 5. In dit hoofdstuk wordt onder andere nader uitgelegd wat Vraagmaatje is en welke gegevensverwerkingen VMC voornemens is te verrichten. Ten slotte worden er in het slothoofdstuk enerzijds conclusies gemaakt door hoofdstuk 3 en 4 aan elkaar te koppelen. Deze conclusies zullen een antwoord vormen op de centrale vraag. Anderzijds worden op basis van deze conclusies aanbevelingen gedaan die VMC kan toepassen op haar startup. Dit zal een praktische uitwerking van de conclusies zijn in de vorm van een checklist en stroomdiagram.

Hoofdstuk 2 Privacy en gegevensbescherming

In dit eerste inhoudelijke hoofdstuk wordt u als lezer allereerst stapsgewijs meegenomen in de ontwikkeling van privacyrecht en gegevensbescherming op verschillende niveaus door de jaren heen. Beginnend bij de Volkstelling van 1971 tot aan de huidige stand van zaken, namelijk de inwerkingtreding van de Algemene verordening gegevensbescherming (AVG). Tevens wordt stilgestaan bij zowel de totstandkoming van deze AVG als die van de Wet bescherming persoonsgegevens (Wbp). Vervolgens worden de belangrijkste veranderingen bij de overgang van Wbp naar AVG in kaart gebracht. Ten slotte komt Big Data als onderwerp van de huidige en vermoedelijk toekomstige gegevensbescherming aan bod.

§ 2.1 Historie van privacy en gegevensbescherming vanuit drie perspectieven

Privacy is met de ontwikkeling van de mensheid al decennialang op wereldwijde schaal een punt van discussie. Men wil enerzijds dat de persoonlijke levenssfeer zo goed mogelijk wordt gewaarborgd door de medemens, overheidsinstanties en particuliere organisaties. Tegelijkertijd wil dezelfde groep burgers een zo veilig mogelijke (digitale) omgeving en zo veel mogelijk verbonden zijn met de rest van de wereld. Dit laatste aspect duidt volgens experts ook wel op de 'privacyparadox': de neiging om privacy belangrijk te vinden, maar er niet of nauwelijks naar te handelen.⁸ Deze tegenstrijdige belangen zorgen voor een publieke strijd waarvan gezegd kan worden dat deze nooit zal worden uitgevochten. Het blijft immers een belangenafweging tussen twee gewenste uiteinden, waarover van beide kanten een onderbouwde opinie kan worden gevormd. In deze lijn kan tevens worden vastgesteld dat privacy wereldwijd een alsmaar groeiende kwestie is. Denk hierbij bijvoorbeeld aan de toenemende behoefte aan vooruitstrevende technieken in de opsporing van verdachten en de bestrijding van terreur⁹.

§ 2.1.1 Nationaal perspectief

De eerste nationale vertolking van privacy als grondrecht werd in 1815 vormgegeven door het verbod op het zonder toestemming binnentreden van iemands woning. Dit verbod valt onder de noemer 'ruimtelijke privacy'. Deze vorm van privacy kan worden omschreven als de fysieke, direct waarneembare bescherming van de persoonlijke levenssfeer, met als doel dat ieder individu zich binnen de eigen vier muren vrijelijk te kunnen bewegen en ontplooiën.¹⁰ Vervolgens werd in 1858 tevens het briefgeheim (in 1983 uitgebreid met het telefoon- en telegraafgeheim) aan de Nederlandse Grondwet toegevoegd.¹¹ Beide grondrechten zijn tegenwoordig terug te vinden als art. 12 en 13 van de Grondwet.

Vanaf de jaren zeventig van de vorige eeuw vond er in Nederland de eerste grote maatschappelijke discussie plaats over een andere vorm van privacy, te weten informatiele privacy. Informatiele privacy richt zich op de bescherming van persoonsgegevens van individuen. Het begon in 1970 met de nieuwe Volkstellingenwet en de voorgenomen Algemene Volkstelling van 1971. Deze wet moest het mogelijk maken om te vragen naar een aantal onderwerpen dat op dat moment relevant was.¹² Ondanks kritische kanttekeningen, gericht op de waarborging van persoonlijke gegevens, van onderzoekers en een aantal politici werd deze wet goedgekeurd. In aanloop naar de Volkstelling ontstond er mede dankzij instellingen zoals het Comité Waakzaamheid Volkstelling (CWV) steeds meer commotie over deze aanstaande gebeurtenis. Nog voordat het CBS haar plannen betreffende de Volkstelling bekend wilde maken, werd er namelijk al gewaarschuwd voor de massaler wordende verzameling van eenieders gegevens als gevolg van deze nieuwe Volkstelling. Dit zorgde voor een groeiend wantrouwen bij burgers, welke werd versterkt door het nieuws dat er voor het eerst computers zouden worden gebruikt bij de verwerking van de

⁸ Klous & Wielaard 2016, p. 37.

⁹ Mede door de aanslagen in New York (2001), Madrid (2004), Londen (2005), Parijs (2015) en Brussel (2016).

¹⁰ Hugo Hendrik Kielman 2010, p. 65.

¹¹ Kranenborg & Verhey 2011, p. 1.

¹² Blessing, *Historisch Nieuwsblad* 2005.

vragenlijsten. Veel mensen vonden het een raar en eng idee dat hun persoonsgegevens digitaal werden opgeslagen en raakten daardoor waakzamer. Hierdoor werd de telling tweemaal uitgesteld en ontstond er uiteindelijk alsnog een groep van 250.000 mensen die weigerden deel te nemen aan de Volkstelling in 1971.

Deze gebeurtenissen hebben op den duur niet alleen bijgedragen aan de afschaffing van de klassieke volkstelling in 1991, maar ook aan een algemeen bewustwordingsproces.¹³ Burgers werden namelijk steeds bewuster van de invloeden die de registraties van persoonsgegevens met zich mee zouden kunnen brengen. Waar gegevensbescherming toen nog een relatief vaag begrip was, kwam er als gevolg van deze gebeurtenissen wetgeving tot stand om persoonsgegevens te beschermen, te weten de Wet Persoonsregistraties (Wpr). Daarbij kwam in 1981 de oprichting van een toezichthouder op dit gebied: de Registratiekamer.¹⁴ Deze werd in 2001 omgedoopt tot het College bescherming persoonsgegevens (CBP) dat ruimere bevoegdheden kreeg en sinds 2015 de Autoriteit Persoonsgegevens (AP) heet.¹⁵ In datzelfde jaar kwam de Wbp als opvolger van de Wpr. Hoe de Wbp tot stand is gekomen wordt kort besproken in § 2.2. Ten slotte is bij de Grondwetsherziening in 1983 de bescherming van de persoonlijke levenssfeer in art. 10 opgenomen. In dit artikel wordt de mogelijkheid gegeven om in nadere wetgeving regels op te nemen over de verwerking van persoonsgegevens.

§ 2.1.2 Internationaal perspectief

Binnen de Raad van Europa trad in 1985 het Verdrag van Straatsburg (VvS) in werking. Dit is een verdrag over de geautomatiseerde verwerking van persoonsgegevens dat in beginsel geldt voor de op wereldwijde schaal aangesloten staten. Hierdoor zijn deze verdragsbepalingen niet 'een ieder verbindend' in de zin van art. 94 Gw en dienen deze eerst op nationaal niveau te worden geïmplementeerd. In Nederland is dit in 1993 gebeurd.¹⁶ Het belang van dit Verdrag is in de loop van de tijd overigens afgenomen, nu deze in 1995 is overvleugeld door de Privacyrichtlijn¹⁷ (zie § 2.2).¹⁸ Naast het VvS werd in 1976 het IVBPR van kracht, met daarin onder andere het belangrijke art. 17 betreffende het recht op bescherming van de persoonlijke levenssfeer. Het IVBPR is een verdrag dat in tegenstelling tot het VvS wel een ieder verbindend is en rechtstreekse doorwerking heeft in nationaal recht. Desondanks wordt er in vergelijking met art. 8 EVRM weinig beroep op art. 17 IVBPR gedaan.¹⁹

§ 2.1.3 Europees perspectief

Op Europees niveau is de belangrijkste bron voor de bescherming van de persoonlijke levenssfeer sinds 1953 geregeld in art. 8 EVRM. Deze bepaling is specifiek gericht op het recht op eerbiediging van het privéleven. Hierbij is door de jaren heen in de rechtspraak van het EHRM nadere invulling gegeven aan het begrip 'privéleven', zo ook door toepassing van de bescherming van persoonsgegevens.²⁰ Een zaak kan aan het EHRM worden voorgelegd wanneer alle nationale middelen zijn uitgeput. Verder geeft art. 16 lid 2 VWEU de bevoegdheid aan het Europees Parlement en de Raad om regels vast te stellen over de bescherming van personen ten aanzien van de verwerking van persoonsgegevens.

§ 2.2 Totstandkoming Wbp en AVG

In 1995 werd bekend dat de EU dat jaar de Privacyrichtlijn in werking zou laten treden. Een richtlijn is een bindend advies van de EU aan lidstaten om hun nationale wetgeving op een vormvrije manier op deze richtlijn te baseren, weliswaar zodat in verschillende lidstaten

¹³ Van Maarseveen, CBS: *Set* 2005, p. 33.

¹⁴ Jan Holvast 2013, p. 9-10.

¹⁵ Kranenborg & Verhey 2011, p. 56 – 57.

¹⁶ *Trb.* 1988, 7.

¹⁷ Richtlijn 95/46/EG.

¹⁸ Kranenborg & Verhey 2011, p. 13 – 15.

¹⁹ Koekkoek 2000, p. 159.

²⁰ Kranenborg & Verhey 2011, p. 19 – 21.

hetzelfde resultaat wordt nagestreefd.²¹ Nederland implementeerde deze richtlijn in 2001 door de invoering van de Wet bescherming persoonsgegevens (Wbp). Daarmee gaf zij tevens uitvoering aan hetgeen waar in art. 10 Grondwet (Gw) naar wordt verwezen. De inhoud van de Wbp is niet alleen voor het grootste deel bepaald door de Richtlijn, maar ook door het zojuist besproken Verdrag van Straatsburg en art. 8 EVRM.

Inmiddels is gebleken dat de Richtlijn niet alleen verouderd is, maar ook niet heeft geresulteerd in de gehoopte consistentie, coherentie en efficiëntie aangaande de bescherming van persoonsgegevens binnen de EU. De veroudering is onder andere te wijten aan de technologische ontwikkelingen sindsdien. Het internet stond toen nog in de kinderschoenen en is inmiddels juist een platform waar privacyrecht een belangrijke positie inneemt. Voornoemde factoren zijn dan ook aanleiding geweest voor de Europese Commissie om in januari 2012 een eerste voorstel te doen om de bestaande privacywetgeving te uniformeren en actualiseren in de vorm van een verordening: de Algemene verordening gegevensbescherming.²² Na deze eerste versie volgden er ruim 4000 voorgestelde wijzigingen en heeft de verordening de gebruikelijke processen in de totstandkoming van Europese regelgeving doorlopen. Uiteindelijk werd in december 2015 de definitieve versie bekendgemaakt, welke in mei 2016 in werking is getreden.²³ Hierbij geldt een implementatieperiode van twee jaar, wat wil zeggen dat organisaties tot 28 mei 2018 hebben om hun werkwijzen hierop af te stemmen. Voor die tijd kunnen zij nog geen sancties op grond van de AVG krijgen. De EU hoopt met de invoering van de AVG een gelijkwaardig niveau van bescherming van persoonsgegevens binnen de lidstaten te bereiken.

Tevens zal vanaf deze datum de Wbp in worden getrokken en de AVG als hoofdzakelijke wettelijke bron van gegevensbescherming dienen. De AVG is zoals gezegd een verordening, wat betekent dat deze bindend is en rechtstreekse werking met dezelfde kracht als nationaal recht heeft.²⁴ Deze hoeft dan ook niet eerst te worden omgezet naar nationaal recht, zoals bij een richtlijn wel nodig is. Wel dienen de bepalingen uit de AVG uitvoering te krijgen in de lidstaten. Derhalve is in Nederland op 9 december jl. een eerste conceptversie van de Uitvoeringswet van de AVG gepubliceerd.²⁵ Deze wet is voornamelijk gericht op realisering van de bepalingen betreffende de bevoegdheden van een nationale toezichthouder (in Nederland: de AP) en nadere invulling geven aan bepalingen van de AVG, voor zover deze hiervoor ruimte biedt.

§ 2.3 Belangrijkste verschillen Wbp en AVG

Een groot aantal aspecten in de AVG zijn niet of nauwelijks veranderd ten opzichte van de Wbp. Desondanks zijn er een aantal belangrijke wijzigingen aan te merken. Het belangrijkste verschil is reeds toegelicht: waar de Wbp is ontstaan uit een nationale omzetting van Richtlijn 95/46/EG, is de AVG rechtstreeks geldig in iedere EU-lidstaat. De AVG biedt nog wel enkele ruimte voor aanvullingen in het nationale recht. Inhoudelijk is er ook het een en ander veranderd. Zo zijn de rechten van betrokkenen versterkt, mede door de toevoeging van het recht om 'vergeten te worden'. Bovendien zijn de verplichtingen en verantwoordelijkheden van verwerkers (voorheen: bewerkers) uitgebreid, onder andere met de verplichting om een register bij te houden van alle verrichte verwerkingen van persoonsgegevens. Daartegenover staat dat de verplichting om melding te maken van een verwerking van persoonsgegevens bij de lokale toezichthouder is komen te vervallen. Tevens is het voortaan in een aantal gevallen verplicht om een functionaris voor gegevensbescherming aan te stellen. Verder zijn er een aantal nieuwe begrippen geïntroduceerd, waaronder 'profilering', 'pseudonimisering' en 'genetische' en 'biometrische' gegevens. Ten slotte worden de bevoegdheden van de

²¹ Artikel 288 VWEU.

²² Edossier I, E120003. Te bereiken via Eerstekamer.nl.

²³ Verordening (EU) 2016/679.

²⁴ Artikel 288 VWEU.

²⁵ Uitvoeringswet Algemene verordening gegevensbescherming. Te bereiken via Internetconsultatie op Overheid.nl

ationale toezichthouders bevordert, alsmede de boetebevoegdheden van deze bestuursorganen. Al deze onderwerpen zullen uitgebreid worden besproken in hoofdstuk 3.

§ 2.4 Huidige en toekomstige gegevensverwerking: Big Data

Inmiddels zijn we op het punt aanbeland dat er geen dag voorbij gaat waarop men een krant openslaat of nieuwspagina opent, zonder een privacy gerelateerd artikel tegen te komen. Hierbij speelt het onderwerp 'Big Data' een grote rol. Big Data kan worden omschreven als 'de grote hoeveelheid gegevens die met behulp van een netwerk van verbindingen en sensoren wordt geleverd, kan worden verzameld en door middel van data-analyses aan elkaar kan worden gekoppeld.'²⁶ Dit sluit aan op het begrip 'profilering' dat in hoofdstuk 3 nadere aandacht krijgt. Big Data speelt een steeds grotere rol binnen de maatschappij, mede doordat het bij steeds meer bedrijven een interessante toevoeging is op hun verdienmodel.²⁷ Zij kunnen met deze data in combinatie met algoritmes²⁸ nieuwe producten en diensten in de markt zetten, hun activiteiten efficiënter organiseren en hun klanten maatwerk bieden.²⁹ Big Data is overigens wat anders dan metadata. Metadata betreft relatief concrete gegevens over eigenschappen van gegevens, die zonder gebruik van technologieën al bruikbaar zijn.

Een bekend, indringend voorbeeld is een Amerikaans gezin waarvan de zestienjarige dochter reclame ontving van Target, speciaal gericht op babyartikelen. De vader van het gezin klaagde bij Target omdat zijn dochter helemaal niet zwanger was. Wat bleek: het computersysteem van Target verwachtte op basis van algoritmes dat de dochter zwanger zou zijn. Waarom? Vrouwen die zwanger zijn kopen vaak shampoo die minder sterk ruikt, omdat hun reukvermogen tijdens de zwangerschap toeneemt. Zo voorspelde Target uiteindelijk correct dat de dochter zwanger bleek te zijn.³⁰ Dit voorbeeld geeft aan hoeveel voorspelkracht een systeem op basis van Big Data kan hebben. Dit soort gevallen zorgen voor weerstand bij burgers, mede gelet op het feit dat burgers niet op de hoogte zijn van de mate waarin hun gegevens worden gebruikt. Er wordt echter ook gesteld dat Big Data, op een beheersbare manier, kan bijdragen aan een betere samenleving.³¹ Big Data kan namelijk ook worden gebruikt op andere gebieden, zoals op het gebied van wetenschap, geneeskunde, verkeersveiligheid en technologie.

²⁶ Klous & Wielaard 2016, p. 16 – 19.

²⁷ Executive Office of the President & PCAST 2014, p. 5 en 22 – 25.

²⁸ Een algoritme is in het kort een wiskundig model waarmee patronen gevonden kunnen worden in grote datasets en die daardoor voorspellende capaciteiten bezit.

²⁹ Klous & Wielaard 2016, p. 46 – 47 en Van Beelen e.a. 2015, p.76.

³⁰ Charles Duhigg, *The New York Times Magazine* 2012.

³¹ Klous & Wielaard 2016, p. 23.

Hoofdstuk 3 Algemene verordening gegevensbescherming

Dit hoofdstuk richt zich op het uitdiepen van het juridisch kader in casu: de Algemene verordening gegevensbescherming. De meest relevante onderwerpen uit de AVG zullen stapsgewijs de revue passeren. Beginnend bij de reikwijdte van de AVG en de beginselen van gegevensverwerking, eerstens gevolgd door de bijzondere verwerking van gevoelige gegevens en de rechten die betrokkenen kunnen uitoefenen ter bescherming van hun persoonsgegevens. Vervolgens komen de verantwoordelijkheden van verwerkingsverantwoordelijken en verwerkers, persoonsgegevensbeveiliging en de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging aan bod. Ten slotte worden de functionaris voor gegevensbescherming en de toezichthoudende autoriteit met haar sanctiebevoegdheden besproken.

§ 3.1 Reikwijdte AVG

Voordat de AVG inhoudelijk kan worden getoetst, dient een zekere afbakening van het toepassingsbereik van de AVG plaats te vinden. Art. 1 t/m 4 AVG zijn hierbij leidend. Deze artikelen zijn ten opzichte van de Wbp niet of nauwelijks gewijzigd.

§ 3.1.1 Natuurlijke personen

Om te beginnen stelt art. 1 dat de regels zich richten op de bescherming van *natuurlijke personen* in verband met de verwerking van persoonsgegevens. Overw. 14 van de Preambule vult dit aan door aan te geven dat de AVG geen betrekking heeft op de verwerking van gegevens over rechtspersonen c.q. ondernemingen. Bovendien geldt de AVG volgens overw. 27 niet voor de verwerking van gegevens van overleden personen.

§ 3.1.2 Materieel en territoriaal toepassingsgebied

Materieel toepassingsgebied

Vervolgens is de AVG volgens art. 2 lid 1 van toepassing op de *geheel of gedeeltelijk geautomatiseerde verwerking*, alsmede de verwerking van persoonsgegevens die in een *bestand* zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Dit is een ruime omschrijving van het materieel toepassingsgebied. Geautomatiseerde verwerking wil zeggen dat er middelen, methoden en/of technologieën worden gebruikt om de verwerking tot stand te laten komen.³² Er is sprake van een gedeeltelijke geautomatiseerde verwerking als gegevens deels geautomatiseerd en deels handmatig worden verwerkt.³³ Van één vorm van verwerking van persoonsgegevens is sprake als geautomatiseerde en niet geautomatiseerde gegevens een gemeenschappelijke bestemming hebben.³⁴ Overw. 15 benadrukt hierbij dat de bescherming technologie-neutraal en niet afhankelijk van gebruikte technologieën dient te zijn. Ook is de AVG van toepassing wanneer het gaat om een puur handmatige verwerking, indien de verwerking gegevens betreft die in een bestand worden opgenomen of daarvoor zijn bedoeld.³⁵ Een bestand is volgens art. 4 onderdeel 6 AVG elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn. (Een verzameling) dossiers die niet volgens specifieke criteria zijn gestructureerd vallen derhalve volgens overw. 15 niet onder het toepassingsgebied van de AVG.

In art. 2 lid 2 AVG zijn een aantal uitzonderingen op het materieel toepassingsgebied opgesomd, zoals bij verwerkingen in het kader van zuiver persoonlijke of huishoudelijke activiteiten (sub c). Deze activiteiten dienen volgens overw. 18 geen enkel verband te houden met beroeps- of handelsactiviteit. Een andere uitzondering geldt voor activiteiten die buiten de werkingssfeer van het Unierecht vallen (sub a). Deze uitzondering dient volgens §

³² Kamerstukken II 1997/98, 25892, 3, p. 69.

³³ Kranenborg & Verhey, p. 59.

³⁴ Kamerstukken II 1997/98, 25892, 3, p. 69.

³⁵ Kamerstukken II 1997/98, 25892, 3, p. 52 – 53.

2.2 MvT UAVG³⁶ beperkt te worden uitgelegd. Het gaat hierbij namelijk uitsluitend om gegevensverwerkingen op terreinen die in hun geheel zijn uitgezonderd van de werking van Europees recht. Daarmee worden, mede gelet op overw. 16 Preambule AVG, verwerkingen in het kader van de nationale veiligheid bedoeld.

Territoriaal toepassingsgebied

Onder de reikwijdte van de AVG valt volgens art. 4 de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke (hierna ook wel te noemen: 'wvv') of een verwerker in de EU, ongeacht of de verwerking al dan niet in de EU plaatsvindt. De AVG is volgens overw. 23 en 24 ook van toepassing op gegevensverwerkingen van betrokkenen die zich in de EU bevinden, door een niet in de EU gevestigde wvv, wanneer de verwerking van persoonsgegevens betrekking heeft op het aanbieden van goederen of diensten aan betrokkenen of voor het observeren van het gedrag van betrokkenen, voor zover dit gedrag in de EU plaatsvindt.

§ 3.1.3 Persoonsgegevens

Naast deze toepassingsgebieden moet worden beoordeeld welke gegevens worden bestempeld als persoonsgegevens in de zin van de AVG. Art. 4 onderdeel 1 geeft aan dat persoonsgegevens alle informatie over een *geïdentificeerde of identificeerbare natuurlijke persoon* betreft. Dit is niet alleen informatie in geschreven tekst, maar ook in beeld en geluid (foto's, filmpjes, geluidsopnamen et cetera).³⁷

Over een persoon

Deze informatie moet gerelateerd zijn aan een individueel natuurlijk persoon. Hiervan is bijvoorbeeld al snel sprake bij directe persoonsgegevens zoals een naam, of bij biometrische gegevens waaronder vingerafdrukken, DNA-profielen, irisscans en iemands stem.³⁸ Dit is echter niet in alle situaties gemakkelijk vast te stellen. In veel gevallen, zoals bij feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen, zal de vaststelling uit de *aard van de gegevens* moeten voortvloeien.³⁹ Dit is bijvoorbeeld het geval bij gegevens die betrekking hebben op een zaak, proces of gebeurtenis. In die gevallen is ook de *context waarin de gegevens worden gebruikt* essentieel en zal aan de hand van de feitelijke situatie moeten worden beoordeeld of er sprake is van persoonsgegevens.

Hoe dan ook dient er een realistische mogelijkheid te zijn dat er een verband kan worden gemaakt tussen een gegeven en een persoon. Zo vallen zuivere objectgegevens volgens voornoemde bronnen buiten dit bereik. Telefoonnummers zijn enkel persoonsgegevens wanneer deze herleidbaar zijn tot een specifiek natuurlijk persoon. Kentekengegevens zijn voor personen zonder toegang tot het kentekenregister geen persoonsgegevens indien redelijkerwijs ook niet te verwachten valt dat die gegevens langs een omweg zullen worden herleid. Ook IP-adressen zijn persoonsgegevens omdat deze kunnen herleiden tot een natuurlijk persoon. Verder geldt in het algemeen dat als gegevens over zaken of gebeurtenissen in verband worden gebracht met personen en in die context medebepalend zijn voor de wijze waarop zij in het maatschappelijk verkeer worden beoordeeld of behandeld, dergelijke gegevens als persoonsgegevens moeten worden aangemerkt.⁴⁰

Identificeerbaar

Bovendien moeten de gegevens betrekking hebben op een geïdentificeerd of identificeerbaar persoon (ook wel: betrokkene). Als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online

³⁶ Uitvoeringswet Algemene verordening gegevensbescherming. Te bereiken via Internetconsultatie op Overheid.nl

³⁷ *Kamerstukken II 1997/98, 25892, 3, p. 50.*

³⁸ Kranenborg & Verhey, p. 60.

³⁹ *Kamerstukken II 1997/98, 25892, 3, p. 46.*

⁴⁰ Kranenborg & Verhey, p. 60.

identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die persoon. Met andere woorden, er moet overwogen worden in hoeverre een gegeven herleidt of kan herleiden tot één specifiek persoon. Directe gegevens zoals naam, adres en geboortedatum zijn in combinatie met elkaar zodanig uniek voor een bepaald persoon dat deze relatief eenvoudig kan worden geïdentificeerd. Hetzelfde geldt voor biometrische gegevens met hun unieke en sterk identificerend karakter.⁴¹

Maar hoe zit het met indirecte gegevens zoals woonplaats, leeftijd, beroep? Uitgangspunt hierbij is de vraag in hoeverre met behulp van een bepaald gegeven op zich, of in combinatie met andere gegevens, de identiteit van een betrokkene zonder *onevenredige inspanning* kan worden vastgesteld. Twee factoren spelen hierbij een rol: de aard van de gegevens en de mogelijkheden van de wv om de identificatie tot stand te brengen. Dit laatste aspect richt zich op de middelen, waaronder tijd, geld, mankracht, expertise, selectietechnieken en technische en technologische faciliteiten, die diegene ter beschikking heeft en redelijkerwijs kan inzetten om een betrokkene te identificeren. Er moet hierbij worden uitgegaan van een redelijk toegeruste wv. Indien een disproportionele inspanning nodig is om een identiteit te achterhalen, is er geen sprake van een persoonsgegeven. Dit is tevens het geval bij anonieme gegevens: gegevens die geen betrekking hebben op een identificeerbaar persoon of zodanig geanonimiseerd zijn dat een betrokkene niet meer identificeerbaar is. Anonimisering kan onder andere aan de orde zijn bij gegevensverwerking voor statistische of onderzoeksdoeleinden.

Een combinatie van beroep, woonplaats en leeftijd is overigens doorgaans sterk identificerend, ook als de identiteit van een betrokkene niet meteen wordt vermeld.⁴² Indien (een combinatie van) gegevens worden gebruikt die een betrokkene minder snel zouden identificeren, zoals leeftijdsklasse, woonregio en beroepsklasse, moet wederom worden gekeken naar de context. Door vergelijking van gegevens en/of koppeling aan gegevens uit andere bronnen, kan immers identificatie tot stand worden gebracht. Dit kan bijvoorbeeld afhankelijk zijn van de omvang van de bevolkingsgroep waarop de gegevensverwerking betrekking heeft.⁴³

Ten slotte laat de AVG in art. 87 ruimte aan de lidstaten om bij wet voorwaarden te stellen aan de verwerking van het nationaal identificatienummer (burgerservicenummer; BSN). Hier wordt uitvoering aan gegeven in art. 38 jo. 44 van de voorlopige UAVG. Art. 38 bepaalt dat het verbod op gegevens waaruit ras of etnische afkomst blijkt (waaronder het BSN), niet geldt voor zover verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting of ter uitvoering van een taak van algemeen belang. Art. 44 stelt daarnaast vast dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts wordt gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. Deze bepaling dient als basis voor verschillende invulling in specifiekere wetten, zoals de Wet algemene bepalingen burgerservicenummer (art. 10 Wabb) en de Wet gebruik burgerservicenummer in de Zorg. De nationale wetgeving betreffende het BSN blijft met de inwerkingtreding van de AVG ongewijzigd.

§ 3.1.4 Verwerking

Nu uitvoerig is behandeld welke gegevens als persoonsgegevens dienen te worden bestempeld, dient in kaart te worden gebracht welke activiteiten onder de noemer 'verwerking' behoren. In art. 4 onderdeel 2 wordt dit begrip gedefinieerd als 'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés'. Hieronder valt het gehele proces van verzameling en gebruik tot aan vernietiging van persoonsgegevens.

⁴¹ Kamerstukken II 1997/98, 25892, 3, p. 46. en Kranenborg & Verhey, p. 61 en 64 – 65.

⁴² Kamerstukken II 1997/98, 25892, 3, p. 47 – 49 en Kranenborg & Verhey, p. 61.

⁴³ Kamerstukken II 1997/98, 25892, 3, p. 48.

Verkrijging van persoonsgegevens is ook verwerking, wat er onder andere voor zorgt dat het doel van een verwerking al voor de verkrijging dient te worden vastgesteld. Ook anonimiseren wordt gezien als een verwerking, omdat dit een vorm van wijzigen of vernietigen van persoonsgegevens kan zijn. Bij een verwerking is het verder belangrijk dat er enige feitelijke macht over de persoonsgegevens kan worden uitgeoefend door de desbetreffende vvv of verwerker. Op het moment dat er geen mogelijkheid bestaat om invloed uit te oefenen op de persoonsgegevens, is er geen sprake van verwerking.⁴⁴

Daarnaast wordt gesproken van een handeling of geheel van handelingen, wat impliceert dat ook een bundeling van verwerkingshandelingen die in het maatschappelijk verkeer als een eenheid wordt beschouwd onder de AVG valt. Een voorbeeld hiervan zou de verzameling, opslag en het gebruik van een bepaald type persoonsgegevens zijn, mits deze tot één doel dienen.⁴⁵ Hierdoor worden een aantal wettelijke verplichtingen van de vvv en verwerker enigszins vergemakkelijkt. Een voorbeeld hiervan is de registerplicht van art. 30 AVG (zie § 3.5), nu een bundeling van verwerkingshandelingen met hetzelfde doel als één verwerking kan worden geregistreerd.

§ 3.2 Beginselen voor verwerking

In art. 5 AVG zijn de beginselen omtrent de verwerking van persoonsgegevens opgesomd. Met deze beginselen moet bij iedere verwerking rekening worden gehouden.

1. Rechtmatigheid, behoorlijkheid en transparantie (art. 5 lid 1 sub a AVG)

Elke verwerking van persoonsgegevens dient te allen tijde *behoorlijk* en *transparant* te geschieden. Het transparantiebeginsel is nieuw ten opzichte van de Wbp en houdt in dat een vvv eerlijk (van het Engelse 'fair') moet zijn over zijn werkwijzen met betrekking tot de verwerking van persoonsgegevens en hierover openheid moet geven. Overw. 39 en 58 Preambule vullen dit beginsel aan door te stellen dat informatie en communicatie in verband met een verwerking eenvoudig toegankelijk en begrijpelijk moet zijn en dat duidelijke en eenvoudige taal moet worden gebruikt. Dit betekent onder andere dat betrokkenen niet alleen moeten worden geïnformeerd over de identiteit van de vvv en over de doeleinden van de verwerking. Zij dienen ook op de hoogte te worden gesteld van hun rechten, zoals het recht op bevestiging en mededeling van de verwerking van hun persoonsgegevens. Dit geldt in het bijzonder voor situaties waarin het voor de betrokkene moeilijk te begrijpen is wie met welk doel zijn persoonsgegevens verwerkt. Een vorm van transparantie kan ook een kort en bondig gegevensbeschermingsbeleid met duidelijke, begrijpelijke privacyvoorwaarden zijn.

In aansluiting op het voorgaande is een vvv volgens overw. 42 verplicht om voorafgaand aan een verwerking een vorm van verklaring van toestemming op te stellen in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. Deze verklaring mag in overeenstemming met Richtlijn 93/13/EEG geen oneerlijke bedingen bevatten. De betrokkene moet ten minste bekend raken met de identiteit van de vvv en de doeleinden van de gegevensverwerking. Verder moet een betrokkene van tevoren worden meegedeeld of hij verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn van niet-verstrekking van de gegevens. Anders gezegd, personen moeten bewust worden gemaakt van de risico's, regels en waarborgen en de mogelijkheden tot uitoefening van hun rechten omtrent de verwerking van persoonsgegevens.

Het *rechtmatigheidsbeginsel* is in tegenstelling tot de voorgaande beginselen concreet: de rechtsgrondslagen zijn limitatief opgesomd in art. 6 sub a t/m f AVG. Een verwerking is enkel rechtmatig indien en voor zover aan ten minste een van deze voorwaarden is voldaan:

- a) de betrokkene heeft *toestemming* gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

⁴⁴ Kamerstukken II 1997/98, 25892, 3, p. 51 – 52.

⁴⁵ Kamerstukken II 1997/98, 25892, 3, p. 51 – 52.

Onder 'toestemming' wordt volgens art. 4 onderdeel 11 AVG verstaan: 'elke vrije, specifieke, geïnformeerde en *ondubbelzinnige* wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt.' Ondubbelzinnig wil zeggen dat er geen twijfel mag zijn over de vraag of betrokkene zijn toestemming heeft verleend.⁴⁶ In een onderzoek van de AP (toen nog CBP) naar het privacybeleid van Google werd nog maar eens gewezen op het belang van het ondubbelzinnigheidsvereiste.⁴⁷ Toestemming mag volgens de bevindingen uit dit onderzoek niet worden verkregen via algemene voorwaarden en niet voortvloeien uit het uitblijven van actie door of het stilzwijgen van een betrokkene. Geconcludeerd werd dat Google zonder toestemming een onzichtbaar web van persoonsgegevens spint. Verder wordt bij de beoordeling van de term 'vrij' volgens art. 7 lid 4 AVG onder meer rekening gehouden met de vraag of voor de uitvoering van een overeenkomst toestemming is vereist voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering ervan. Met andere woorden, er geldt een zwaardere toetsingsnorm voor de toestemming als er sprake is van de uitvoering van een overeenkomst en het gaat om een verwerking die hier niet noodzakelijk voor is.

De memorie van toelichting (MvT) op de Wbp heeft destijds drie essentiële punten opgesteld over de toestemming.⁴⁸ De betrokkene moet ten eerste in vrijheid zijn wil kunnen uiten en niet onder druk worden gezet. Hierbij moet rekening worden gehouden met art. 3:33 en 3:35 BW (wil en gerechtvaardigd vertrouwen) en met situaties waarin een duidelijke wanverhouding bestaat tussen vvv en betrokkene. Dit laatste zou er namelijk voor kunnen zorgen dat de betrokkene geen echte of vrije keuze heeft gehad of het verzoek om toestemming niet kan weigeren. Voorbeelden hiervan zijn situaties tussen betrokkenen en overheidsinstanties of werkgevers. Ten tweede geldt dat wilsuiting van de betrokkene specifiek betrekking moet hebben op een concrete verwerking of een beperkte categorie van verwerkingen. Ten derde moet rekening worden gehouden met de *informed consent*: de betrokkene moet goed en volledig zijn ingelicht over de verwerking, alvorens hij zijn toestemming verleent. Desondanks heeft een betrokkene volgens de MvT tot op zekere hoogte zelf een onderzoeksplicht.

Art. 7 AVG stelt naast het zojuist genoemde lid 4 nog andere formaliteiten omtrent de toestemming, zoals de eis in lid 1 dat de vvv aan moeten kunnen tonen dat de betrokkene toestemming heeft gegeven voor een verwerking. Lid 2 richt zich op een toestemming die meerdere aangelegenheden betreft. In dat geval moet het verzoek om toestemming zo worden gepresenteerd dat een duidelijk onderscheid kan worden gemaakt tussen de verschillende zaken. Ook moet er volgens overw. 42 Preambule in een dergelijke situatie extra op worden gelet dat een betrokkene zich ervan bewust is dat hij toestemming geeft en hoever deze toestemming reikt. Verder heeft een betrokkene volgens lid 3 te allen tijde het recht zijn toestemming zonder nadelige gevolgen in te trekken op een wijze die even eenvoudig is als het geven ervan. Ten slotte is volgens art. 8 lid 1 bij een rechtstreeks aanbod van diensten via internet (art. 3:15d lid 3 BW) aan een kind van jonger dan 16 jaar toestemming c.q. machtiging vereist van de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt.

- b) de verwerking is noodzakelijk voor de *uitvoering van een overeenkomst* waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
Deze grond geldt in (pre)contractuele situaties waarbij een betrokkene partij is. Dergelijke gegevensverwerkingen worden doorgaans toelaatbaar geacht, omdat de

⁴⁶ Kranenborg & Verhey, p. 85.

⁴⁷ College bescherming persoonsgegevens 2013, p. 3 – 4.

⁴⁸ *Kamerstukken II 1997/98, 25892, 3, p. 65 – 68.*

betrokkene bij deze gevallen invloed heeft op de verwerking van zijn gegevens.⁴⁹ Het kan hier bijvoorbeeld gaan om naw-gegevens die nodig zijn om de betrokkene te identificeren.

- c) de verwerking is noodzakelijk om te voldoen aan een *wettelijke verplichting* die op de verwerkingsverantwoordelijke rust;
Deze rechtsgrond dient een grondslag te hebben in nationaal of Europees recht, die als basis dient voor verscheidene verwerkingen op grond van deze voorwaarde. De term 'wettelijke verplichting' heeft betrekking op iedere verplichting tot gegevensverwerking die krachtens een algemeen verbindend voorschrift wordt opgelegd. Een dergelijke bepaling hoeft geen uitdrukkelijke opdracht te geven tot verwerking. Wel is van belang dat er een evident verband bestaat tussen de verwerking en uitvoering van de wettelijke verplichting.⁵⁰ Een voorbeeld van een verwerking op deze grond is het verschaffen van informatie door bestuursorganen op grond van de Wet openbaarheid van bestuur. Ondanks het bestaan van een wettelijke verplichting, dient de verwerking proportioneel te zijn.
- d) de verwerking is noodzakelijk om de *vitale belangen* van de betrokkene of van een andere natuurlijke persoon te beschermen;
Hierbij gaat het doorgaans om een verwerking waarvoor dringende medische noodzaak nodig is en het vragen van toestemming redelijkerwijs niet mogelijk is.⁵¹
- e) de verwerking is noodzakelijk voor de vervulling van een *taak van algemeen belang* of van een taak in het kader van de uitoefening van het *openbaar gezag* dat aan de verwerkingsverantwoordelijke is opgedragen;
Deze voorwaarde is bedoeld om gegevensverwerking mogelijk te maken voor de publieke sector (overheid). Een taak is publiekrechtelijk indien deze is gebaseerd op een speciaal voor het openbaar bestuur bij of krachtens de wet geschapen grondslag.⁵²
- f) de verwerking is noodzakelijk voor de behartiging van de *gerechtvaardigde belangen* van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.
Dit is de restgrondslag ten opzichte van de andere grondslagen. Van belang is dat naast het noodzakelijkheidscriterium een belangenafweging plaatsvindt tussen de belangen van de verwerking en die van een betrokkene, rekening houdend met de redelijke verwachtingen van de betrokkene. Een voorbeeld hiervan is als hij verwacht dat zijn persoonsgegevens niet verder worden verwerkt. Net als bij de toestemming geldt hierbij dat er een relevante en passende verhouding bestaat tussen betrokkene en vww, zoals in situaties waarin de betrokkene zijn klant of werknemer is. Al met al dient goed gemotiveerd te worden wat de verwerking noodzakelijk maakt en waarom het belang hiervan, zoals het belang om in goede uitoefening van een bedrijf de noodzakelijke gegevens te verwerken, boven de belangen van een betrokkene geplaatst dienen te worden.

Zoals af te lezen uit de bepaling moet er extra rekening worden gehouden met kinderen. Zij hebben volgens overw. 38 Preambule recht op specifieke bescherming van hun persoonsgegevens, aangezien zij zich doorgaans minder bewust zijn van de mogelijke risico's, gevolgen en waarborgen en van hun rechten. Deze bescherming geldt des te meer in situaties waar persoonsgegevens worden verwerkt voor

⁴⁹ Kranenborg & Verhey, p. 86.

⁵⁰ Kamerstukken II 1997/98, 25892, 3, p. 82 – 83.

⁵¹ Kamerstukken II 1997/98, 25892, 3, p. 84.

⁵² Kamerstukken II 1997/98, 25892, 3, p. 84.

marketingdoeleinden, waarbij profielen worden opgesteld van betrokkenen of waarbij het gaat om gebruik van rechtstreeks aan kinderen verstrekte diensten.

Bij de voorwaarden die de term '*noodzakelijk*' bevatten dient een proportionaliteits- en subsidiariteitstoets te geschieden. De inbreuk op het belang of recht van een betrokkene mag door een bepaalde verwerking niet onevenredig zijn in verhouding tot het doel van die verwerking.⁵³ Beoordeeld moet worden of de verwerking weliswaar plaats moet vinden dan wel of het doel van de verwerking niet op een andere wijze kan worden verwezenlijkt of er voor de verwerking geen andere, minder ingrijpende mogelijkheid openstaat, zoals geanonimiseerde verwerking van de persoonsgegevens.

2. Doelbinding en onverenigbaar gebruik (art. 5 lid 1 sub b AVG)

Persoonsgegevens moeten volgens *welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden* worden verzameld en mogen vervolgens niet verder op een met die doeleinden *onverenigbare wijze* worden verwerkt. Voorheen waren deze beginselen geregeld in art. 7 en 9 Wbp. De doeleinden dienen expliciet en gerechtvaardigd te zijn en te zijn vastgesteld voorafgaand aan de verwerking. Met 'gerechtvaardigd' wordt bedoeld: in overeenstemming met een van de voorwaarden van art. 6 AVG. Ondanks deze vereiste, precieze doelomschrijving mogen de betreffende gegevens ook voor andere doeleinden worden gebruikt dan aanvankelijk bedoeld, mits de doeleinden voor deze verdere verwerking verenigbaar zijn met het oorspronkelijke doel.⁵⁴ Dit heet ook wel de *function creep*: er vindt een andere, onverwachte uitwerking plaats dan in eerste instantie bedoeld. Voorbeelden van verdere verwerking zouden kunnen zijn het verstrekken van de betreffende gegevens aan derden of het creëren van een nieuwe verwerking door verschillende soorten gegevens te koppelen.

Bij het beginsel van verenigbaar gebruik dient een vww volgens art. 6 lid 4 AVG onder meer rekening te houden met de verbanden tussen de doeleinden van de aanvankelijke en voorgenomen verdere verwerking en met het kader waarin de gegevens zijn verzameld, met name gelet op de redelijke verwachtingen van betrokkenen betreffende het verdere gebruik op basis van de bestaande verhouding. Dit laatstgenoemde element heeft betrekking op het idee dat een doel dat nauw samenhangt met de aanvankelijke verwerking, doorgaans aansluit bij het verwachtingspatroon van een betrokkene.⁵⁵ Verder dient een vww de aard van de persoonsgegevens, de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen en bestaande passende waarborgen bij de verwerkingen in beschouwing te nemen. Deze aspecten gelden niet wanneer de oorspronkelijke verwerking heeft plaatsgevonden met *toestemming* als wettelijke grondslag. In dat geval moet de vww de mogelijkheid krijgen tot verdere verwerking, ongeacht eventueel onverenigbaar gebruik. Desondanks dienen volgens overw. 50 de beginselen te worden toegepast en dient de betrokkene te worden geïnformeerd over het doel van de verdere verwerking en over zijn rechten hierbij, waaronder het recht op bezwaar.

3. Dataminimalisatie (minimale gegevensverwerking) (art 5 lid 1 sub c AVG)

Wat mij betreft zou dit beginsel ook wel '*dataoptimalisatie*' kunnen worden genoemd. Persoonsgegevens moeten namelijk *toereikend* zijn, *ter zake dienend* en *beperkt* tot wat *noodzakelijk* is voor de doeleinden waarvoor zij worden verwerkt. Dit beginsel was in de Wbp opgenomen als art. 11 en vergt net als bij de beginselen een proportionaliteitstoets. 'Toereikend' betekent hier dat het noodzakelijk is om gelet op het doel van de verwerking, te beschikken over voldoende informatie. Het is namelijk van belang dat er geen ongunstig beeld ontstaat van een betrokkene als gevolg van onvolledige informatie, waardoor deze betrokkene schade kan lijden.⁵⁶ Dit is gezien art. 11 AVG niet noodzakelijk indien het doel van een verwerking niet (meer) vereist dat een betrokkene geïdentificeerd wordt.

⁵³ Kranenborg & Verhey, p. 84.

⁵⁴ Kranenborg & Verhey, p. 93.

⁵⁵ Kranenborg & Verhey, p. 93 en *Kamerstukken II 1997/98*, 25892, 3, p. 89-94.

⁵⁶ Kranenborg & Verhey, p. 97.

Tegelijkertijd mogen er niet meer persoonsgegevens worden verwerkt dan met het oog op het betreffende doel nodig is. Ter zake dienend wil zeggen dat bij een verwerking de gegevens moeten worden verwerkt die noodzakelijk zijn voor het aangaande doel. Met andere woorden, het gaat er niet puur om of er te veel of te weinig gegevens van een betrokkene aanwezig zijn, maar juist of de hoeveelheid aanwezige gegevens in optimale verhouding staat tot het doel van de betreffende verwerking.

4. Opslagbeperking (art 5 lid 1 sub d AVG)

Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkene niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is. Dit beginsel was voorheen vastgelegd in art. 10 Wbp. De opslagperiode dient daarom te worden beperkt tot een strikt minimum en er moeten termijnen worden vastgesteld voor het wissen van gegevens of voor een periodieke toetsing ervan. Zodra het beoogde doel van de verwerking is bereikt moet de verwerking in beginsel worden beëindigd.⁵⁷ Voor gegevensverwerkingen met historische, statistische of wetenschappelijke doeleinden overeenkomstig art. 89 lid 1 AVG geldt dat persoonsgegevens langer mogen worden opgeslagen dan verwerkingen met andere doelen.

5. Juistheid (art 5 lid 1 sub e AVG)

Persoonsgegevens moeten *juist zijn* en zo nodig moeten alle redelijke maatregelen worden genomen om deze te actualiseren, rectificeren of verwijderen. Deze maatregelen zouden bijvoorbeeld genomen kunnen worden door toepassing van de zojuist besproken periodieke toetsing. Daarnaast moet een betrokkene in staat worden gesteld om zijn rechten makkelijker uit te oefenen, zoals door mechanismen om verwijdering van zijn gegevens te verzoeken. Dit wordt nader besproken in § 3.4.

6. Integriteit en vertrouwelijkheid (art 5 lid 1 sub f AVG)

Persoonsgegevens moeten door het nemen van passende fysieke, technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een *passende beveiliging* ervan gewaarborgd is. Ook moeten deze gegevens én de gebruikte apparatuur beschermd zijn tegen ongeoorloofd of onrechtmatig gebruik en tegen onopzettelijk verlies, vernietiging of beschadiging. Deze bepaling komt grotendeels overeen met art. 13 en 14 Wbp. Bij technische maatregelen kan worden gedacht aan de logische en fysieke maatregelen in en rondom de informatiesystemen, toegangscontroles en vastlegging van gebruik door back-ups. Organisatorisch doelt op maatregelen voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens, zoals toekenning van en verdeling van bevoegdheden aan vzw's, instructies, trainingen en calamiteitenplannen.⁵⁸

§ 3.3 Bijzondere verwerking

Er zijn een aantal categorieën bijzonder gevoelige persoonsgegevens die worden aangeduid als *bijzondere verwerkingen* en in beginsel verboden zijn. Deze categorieën worden genoemd in art. 9 lid 1 AVG. Het betreft de verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken. Ook valt hieronder de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid of met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Ten opzichte van de Wbp worden genetische en biometrische gegevens voortaan geclassificeerd als bijzondere persoonsgegevens. Genetische gegevens zijn volgens § 4.3 UAVG gegevens met betrekking tot iemands genen. Biometrische gegevens zijn volgens de UAVG exacte, universele, unieke, permanente meetgegevens over personen, zoals een netvlies, iris, gezichtsherkenning, stem en vingerafdruk. Foto's worden slechts onder bepaalde omstandigheden aangemerkt als biometrische gegevens, zoals

⁵⁷ Kranenborg & Verhey, p. 100.

⁵⁸ Kranenborg & Verhey, p. 98.

wanneer foto's worden verwerkt met betrekking tot technische middelen die de unieke identificatie van een persoon mogelijk maken. Daardoor worden foto's niet systematisch beschouwd als verwerking van bijzondere gegevens, maar is de context van de verwerking relevant.⁵⁹

De verwerking van gevoelige gegevens is wel toegestaan op een van de in lid 2 genoemde uitzonderingen. De belangrijkste uitzondering is wanneer de betrokkene zijn uitdrukkelijke toestemming heeft gegeven, tenzij nationaal recht deze uitzondering opheft. Hiervan is in ieder geval in de voorlopige UAVG vooralsnog geen sprake. Andere genoemde uitzonderingen zijn verwerkingen die betrekking hebben op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt (sub e) of verwerkingen die worden verricht door een organisatie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is (d). Ook verwerkingen die noodzakelijk zijn met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig art. 89 lid 1 zijn niet verboden (j).

In lid 2 wordt bij verschillende uitzonderingen de mogelijkheid geboden om hiervan in nationaal recht af te wijken. Ook art. 9 lid 4 AVG biedt mogelijkheden voor lidstaten om bijkomende voorwaarden c.q. beperkingen te verbinden aan de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid. Van deze ruimte wordt in de voorlopige UAVG gebruikgemaakt in art. 22 t/m 31. Zo wordt bepaald dat het verbod op verwerking van gegevens met betrekking tot ras of etnische afkomst niet van toepassing is met het oog op identificatie van de betrokkene en slechts voor zover dit voor het betreffende doel onvermijdelijk is. Ook is het verwerkingsverbod met betrekking tot gezondheid niet van toepassing indien de verwerking geschiedt door bepaalde personen of instanties zoals hulpverleners, verzekeraars, scholen et cetera. Het verbod op verwerking van genetische gegevens is niet van toepassing indien een zwaarwegend geneeskundig belang prevaleert. Verder is het verbod om biometrische gegevens te verwerken met het oog op de unieke identificatie van een persoon niet van toepassing indien de verwerking geschiedt met het oog op de identificatie van de betrokkene en slechts voor zover dit voor dit doel noodzakelijk en proportioneel is.

Strafrechtelijke gegevens worden niet aangemerkt als bijzondere persoonsgegevens, maar worden wel in een apart artikel genoemd: art. 10 AVG. Dit artikel bepaalt dat verwerking van desbetreffende gegevens moet plaatsvinden onder begeleiding van de overheid, tenzij nationaal recht anders bepaalt. Art. 31 lid 1 UAVG geeft een aantal situaties weer waarin strafrechtelijke gegevens ook mogen worden verwerkt. Een voorbeeld hiervan is de situatie waarin een vvv deze gegevens ten eigen behoeve verwerkt ter beoordeling van een verzoek van een betrokkene om een beslissing over hem te nemen of om aan hem een prestatie te leveren. Hierbij kan worden gedacht aan een gerechtelijke instantie of een advocaat die een cliënt bijstaat na een verzoek om zijn belangen te laten behartigen.

§ 3.4 Rechten betrokkenen

Een betrokkene komt op grond van de AVG een aantal rechten toe, teneinde dat deze invloed kan uitoefenen op de verwerking van zijn persoonsgegevens. Deze rechten zullen hieronder worden benoemd en uitgelegd:

- Recht op transparante informatie en communicatie en toegang tot persoonsgegevens (art. 12 t/m 14 AVG): een vvv is verplicht passende maatregelen te nemen opdat de betrokkene de informatie en communicatie in verband met de verwerking van zijn persoonsgegevens als bedoeld in art. 13 en 14 in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt. Bovendien dient de vvv de uitoefening van de rechten van een betrokkene

⁵⁹ Overw. 51 AVG.

te faciliteren en mag hij een verzoek hiertoe niet weigeren. Een uitzondering hierop bestaat wanneer de vvv kan aantonen dat hij een betrokkene niet kan identificeren, zoals beschreven in art. 11 AVG. De vvv moet de betrokkene hiervan indien mogelijk in kennis stellen.

Daarnaast bepaalt art. 12 lid 3 dat een vvv uiterlijk binnen een maand dient te reageren op een verzoek van betrokkene om een van zijn rechten uit te oefenen met daarin informatie over het gevolg dat aan het verzoek is gegeven. Deze termijn kan, afhankelijk van het aantal verzoeken en de complexiteit ervan, met twee maanden worden verlengd. De vvv moet dit binnen één maand na ontvangst van het verzoek melden bij de betrokkene. Indien een vvv er niet in slaagt om binnen één maand, na eventuele verlenging binnen drie maanden, te reageren op het verzoek, dient hij binnen één maand na het verzoek de betrokkene mede te delen wat de reden hiervoor is en informeert hij hem over zijn mogelijkheden om een klacht in te dienen bij de nationale toezichthouder en beroep in te stellen bij de rechter. De informatie en communicatie dient kosteloos te geschieden, tenzij het verzoek kennelijk ongegrond of buitensporig is. In dat geval mag een vvv een redelijke vergoeding aanrekenen ten behoeve van administratiekosten of mag hij weigeren gevolg te geven aan het verzoek. De bewijslast hiervoor ligt bij de vvv. Verder is een vvv bij twijfel over de identiteit van betrokkene bevoegd te verzoeken om aanvullende informatie die nodig is ter bevestiging van de identiteit.

In art. 13 en 14 zijn een aantal gegevens opgesomd die een vvv dient te verstrekken aan een betrokkene wanneer zijn persoonsgegevens bij de betrokkene worden verzameld en wanneer deze niet van de betrokkene zijn verkregen. Indien de gegevens bij een betrokkene worden verzameld, verstrekt de betrokkene al bij verkrijging van de gegevens informatie over onder andere: de identiteit van de vvv en eventueel van de functionaris voor gegevensbescherming (hierna: FG; zie § 3.8), over de verwerkingsdoeleinden en over de gerechtvaardigde belangen indien sprake is van art. 8 lid 1 sub f AVG. Ook heeft een betrokkene in dat geval recht op informatie over: de periode gedurende welke de gegevens zullen worden opgeslagen, het feit dat de betrokkene recht heeft de vvv te verzoeken om inzage, rectificatie, wissing en beperking van zijn persoonsgegevens, alsmede het recht bezwaar te maken tegen de verwerking (zie het vervolg van deze paragraaf) en wanneer de verwerking is gebaseerd op art. 6 lid 1 sub a of art. 9 lid 2 sub a het recht heeft zijn toestemming in te trekken. Verder moet de vvv melden dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit en deze mededelen wat de mogelijke gevolgen zijn van het niet verstrekken van gegevens naar aanleiding van een wettelijke of contractuele verplichting. Ten slotte moet informatie worden verstrekt over het bestaan en de verwachte gevolgen van geautomatiseerde besluitvorming, waaronder profilering.⁶⁰

In het geval dat persoonsgegevens niet van de betrokkene zelf zijn verkregen, moet vrijwel dezelfde informatie worden verstrekt. Er zijn een aantal extra gegevens die moeten worden verstrekt, te weten informatie over de betrokken categorieën van persoonsgegevens en over de bron waar de persoonsgegevens vandaan komen, alsmede eventueel of zij afkomstig zijn van openbare bronnen. In dit geval hoeft er echter geen informatie te worden verstrekt over de gevolgen van het niet verstrekken van gegevens naar aanleiding van een wettelijke of contractuele verplichting, omdat een betrokkene hierbij immers partij dient te zijn. Derhalve zullen deze gegevens enkel afkomstig zijn van betrokkene zelf. Bij deze vorm van gegevensver verkrijging is een vvv volgens art. 14 lid 3 verplicht alle besproken informatie binnen een redelijke termijn, doch uiterlijk binnen één maand na verkrijging te verstrekken. Bij beide

⁶⁰ Profilering is elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd.

vormen geldt overigens dat de verplichte informatieverstrekking niet van toepassing is indien en voor zover de betrokkene reeds over deze informatie beschikt.

- Recht op inzage (art. 15 AVG): de betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitend te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens en van nadere informatie die is gericht op een van de in de lid 1 genoemde onderdelen. Hieronder valt onder andere informatie over de verwerkingsdoeleinden, betrokken categorieën van persoonsgegevens en ontvangers aan wie gegevens zijn of zullen worden verstrekt. Ook kan het hierbij gaan om informatie over de periode gedurende welke de gegevens naar verwachting worden opgeslagen en anders de criteria om die termijn te bepalen. Ten slotte betreft het hier informatie over het feit dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit (hier: AP), over alle beschikbare informatie over de bron van de gegevens en over het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in art. 22 lid 1 t/m 4 bedoelde profilering (zie recht op transparante informatie). Indien sprake is van dit laatste aspect, dient nuttige informatie te worden gegeven over de onderliggende logica, alsmede over het belang en de verwachte gevolgen van die verwerking voor de betrokkene. De wv is verplicht de betrokkene na verzoek een kopie van de persoonsgegevens die worden verwerkt te verstrekken, aldus lid 3.
- Recht op rectificatie (art. 16 AVG): de betrokkene heeft het recht om van de wv *onverwijld rectificatie* van hem betreffende onjuiste persoonsgegevens te verkrijgen. Ook heeft hij het recht onvolledige persoonsgegevens te vervolledigen, bijvoorbeeld door een aanvullende verklaring te verstrekken.
- Recht op gegevenswissing (recht op vergetelheid; art. 17 AVG): de betrokkene heeft het recht een wv te verzoeken om *zonder onredelijke vertraging* over te gaan tot *wissing* van hem betreffende persoonsgegevens. Een wv is in sommige gevallen in ieder geval verplicht persoonsgegevens te wissen, namelijk wanneer een van de in lid 1 genoemde gevallen van toepassing is:
 - a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verwerkt;
 - b) de betrokkene trekt zijn toestemming in en er is geen andere rechtsgrond voor de verwerking;
 - c) de betrokkene maakt volgens art. 21 bezwaar tegen de verwerking en zijn belangen prevaleren boven de dwingende gerechtvaardigde gronden voor de verwerking van een wv;
 - d) de persoonsgegevens zijn onrechtmatig verwerkt (zie § 3.2);
 - e) de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op de wv rust volgens nationaal of Europees recht;
 - f) de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij (op internet).

Volgens lid 2 is een wv bij openbaarmaking van gegevens in de online omgeving (bijvoorbeeld Google), met inachtneming van de beschikbare middelen en technologieën, verplicht de wv's die de betreffende persoonsgegevens verwerken op de hoogte te stellen van het verzoek tot wissing van links naar, kopieën of reproducties van die gegevens. Stel: na een zoekopdracht in Google komt de naam van een betrokkene meerdere keren op een negatieve manier als resultaat voor. Na

een verzoek tot wissing bij Google dient zij de websites waarop de naam voorkomt met inachtneming van voornoemde afweging op de hoogte te stellen van het verzoek. Lid 3 geeft nog een aantal gevallen waarbij lid 1 niet van toepassing is, waaronder voor zover de verwerking nodig is voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie. Dit is zoals al vaker gezien wederom een belangenafweging.

- Recht op beperking van de verwerking (art. 18 AVG): de betrokkene heeft het recht om de verwerking van zijn persoonsgegevens te laten *beperken* door een vvv, indien een van de elementen uit lid 1 van toepassing is. Zo heeft een betrokkene recht op beperking gedurende de periode waarin hij de juistheid van zijn gegevens heeft betwist of dat hij bezwaar heeft gemaakt tegen een verwerking. Ook geldt dit recht wanneer de verwerking onrechtmatig is en de betrokkene zich verzet tegen het wissen van de persoonsgegevens en in plaats daarvan verzoekt om beperking van het gebruik ervan. Na een beperking van de verwerking worden de betreffende persoonsgegevens alleen verwerkt, met uitzondering van de opslag, met toestemming van de betrokkene. Indien de betrokkene het recht op beperking heeft verkregen, wordt hij door de vvv ervan op de hoogte gebracht wanneer de verwerking wordt opgeheven.
- Recht op overdraagbaarheid van gegevens (dataportabiliteit; art. 20 AVG): de betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een vvv heeft verstrekt, in een gestructureerde, gangbare, machineleesbare, interoperabele vorm *te verkrijgen*. Ook heeft hij het recht die gegevens aan een andere vvv *over te dragen*, indien de verwerking berust op toestemming of op een overeenkomst (art. 6 lid 1 sub a en b AVG) of als de verwerking geschiedt via geautomatiseerde processen. Machineleesbaar wil zeggen dat het apparaat waar de gegevens naar worden gestuurd deze leesbaar kan tonen. Interoperabel betekent dat de systemen van betrokkene en vvv onderling informatie uit kunnen wisselen. Verder dient een vvv, indien dit technisch mogelijk is, op verzoek van betrokkene persoonsgegevens rechtstreeks naar een andere vvv door te zenden.
- Recht van bezwaar (art. 21 AVG): de betrokkene heeft te allen tijde het recht om *vanwege met zijn specifieke situatie verband houdende redenen* bezwaar te maken tegen de verwerking van zijn persoonsgegevens op basis van art. 6, lid 1, sub e (taak van algemeen belang of uitoefening van het openbaar gezag) of f (gerechtvaardigde belangen vvv) van art. 6, lid 1 of op basis van direct marketing, alsmede profilering op basis van deze bepalingen (zie recht op transparante informatie en communicatie in § 3.4). De vvv is in die gevallen verplicht de verwerking van de persoonsgegevens te staken, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen van de betrokkene. Direct marketing is de directe vorm van aanbieden van producten of diensten door bedrijven.
- Recht om niet te worden onderworpen aan een besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking, waaronder profilering, waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft (art. 22 AVG). Dit geldt niet wanneer het besluit noodzakelijk is voor de uitvoering van een overeenkomst of berust op de uitdrukkelijke toestemming van de betrokkene. Als een van deze twee uitzonderingen van toepassing is, is de vvv verplicht passende maatregelen te nemen ter bescherming van de rechten van betrokkene, waaronder het recht op menselijke tussenkomst en om zijn standpunt kenbaar te maken. Geautomatiseerde besluitvorming en profilering gebaseerd op bijzondere categorieën van persoonsgegevens mogen uitsluitend op specifieke voorwaarden worden toegestaan. Hierbij moeten, gelet op de gevoeligheid van de gegevens, passende maatregelen worden genomen om de rechten van een betrokkene te beschermen.

Ten slotte dient een betrokkene, zoals reeds aangegeven bij § 3.2 onderdeel 5, in staat te worden gesteld om zijn rechten makkelijker uit te oefenen, zoals door mechanismen die het voor hem mogelijk maken te verzoeken om bijvoorbeeld inzage in en rectificatie of wissing van zijn persoonsgegevens, alsmede het bezwaar maken tegen een verwerking. Het verzoek van de betrokkene is overigens vrijwel vormvrij, voor zover duidelijk is om welke betrokkene het gaat en hij duidelijk aangeeft waar hij precies om verzoekt. Bovendien dient de vvv alle redelijke maatregelen te nemen om de identiteit van een betrokkene die inzage verzoekt te controleren. Ten slotte mag een vvv persoonsgegevens niet uitsluitend bewaren om op eventuele verzoeken te reageren.⁶¹

§ 3.5 Verantwoordelijkheden verwerkingsverantwoordelijke en verwerker

Naast de rechten van betrokkenen die een vvv moet waarborgen, heeft een vvv ook zelf nog een aantal verplichtingen. De eerste is de verantwoordingsplicht zoals vastgelegd in art. 5 lid 2 AVG: hij is verantwoordelijk voor de naleving van de in § 3.2 genoemde beginselen en hij moet dit kunnen aantonen. Daarnaast bevatten art. 24 t/m 34 AVG een aantal verplichtingen. Zo dient een vvv volgens art. 24 passende technische en organisatorische maatregelen te treffen (zie ook § 3.2 onderdeel 5) om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen moeten worden geëvalueerd en indien nodig geactualiseerd. Een passend gegevensbeschermingsbeleid is een voorbeeld van een dergelijke maatregel. Maatregelen kunnen onder andere worden aangetoond door aan te sluiten bij goedgekeurde gedragscodes (art. 40 AVG) of gebruik van goedgekeurde certificeringsmechanismen (art. 42 AVG). Voorbeelden van dergelijke gedragscodes zijn de gedragscode voor financiële instellingen en die voor zorgverzekeraars. Daarnaast bestaat er een certificaat voor specifieke rechtmatige gegevensverwerkingen (privacycertificaat). Meer informatie hierover is beschikbaar op de website van de AP.⁶²

Gegevensbescherming door ontwerp en door standaardinstellingen: een vvv is overeenkomstig art. 25 lid 1 tevens verplicht om zowel bij de bepaling van de verwerkingsmiddelen (privacy by design) als bij de verwerking zelf, passende technische en organisatorische maatregelen te treffen. Een voorbeeld hiervan is *pseudonimiseren* (zie § 3.6). Deze maatregelen moeten worden opgesteld met inachtneming van de verwerkingsbeginselen, waaronder het beginsel van minimale gegevensverwerking. Met andere woorden, voortaan dient gedurende het gehele proces van de ontwikkeling van een informatiesysteem, met nadruk op de beginfase, rekening gehouden te worden met de waarborging van persoonsgegevens.

Ook treft een vvv conform lid 2 zulke maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Een voorbeeld van een dergelijke maatregel is om als vvv uit te gaan van standaardinstellingen betreffende privacy, die zo veel mogelijk ten gunste van een betrokkene zijn (privacy by default). Dit is onder andere mogelijk door gebruik te maken van opt-ins, waarbij iemand toestemming moet geven om bijvoorbeeld aangemeld te zijn voor het ontvangen van e-mails en hier niet al bij voorbaat automatisch aangemeld voor te zijn. Andere maatregelen zijn om informatie over gegevensverwerking duidelijk en transparant over te brengen en om privacyvriendelijk beleid ten gunste van de betrokkene op te stellen. Een uitgangspunt bij deze verplichting is om gegevens niet te delen.

⁶¹ Overw. 62 Preamble AVG.

⁶² Certificaat voor rechtmatige verwerking van persoonsgegevens, [Autoriteitpersoonsgegevens.nl](https://autoriteitpersoonsgegevens.nl).

Meerdere verwerkingsverantwoordelijken (art. 26 AVG): wanneer twee of meer vvv's gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke vvv's. Zij stellen op transparante wijze hun verantwoordelijkheden vast.

Verwerker (art. 28 AVG): wanneer een verwerking namens een vvv wordt verricht, doet de vvv uitsluitend een beroep op verwerkers die gepaste garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen die de verwerking aan de vereisten van de AVG laat voldoen en de bescherming van de rechten van de betrokkene waarborgt. Een verwerker is vrijwel altijd een instelling of persoon die zich buiten de organisatie van de vvv bevindt en die niet in hiërarchische relatie tot hem staat. Daar waar een hiërarchische relatie bestaat met de verantwoordelijke moet worden gesproken van (intern) beheer.⁶³ De verwerking door een verwerker wordt geregeld in een overeenkomst die de verwerker ten aanzien van de vvv bindt. Deze overeenkomst heet een 'verwerkersovereenkomst' (voorheen: bewerkersovereenkomst) en bevat afspraken over hoe de verwerker dient om te gaan met de verwerking van persoonsgegevens. Een voorbeeld hiervan is op welke wijze en hoelang welke gegevens worden verwerkt en hoe de verwerker omgaat met een datalek (zie § 3.6).

Register van verwerkingsactiviteiten (art. 30 AVG): elke vvv houdt een schriftelijk of elektronisch register bij van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. Dat register bevat alle in lid 1 genoemde gegevens, te weten: de naam en contactgegevens van de vvv en FG, de verwerkingsdoeleinden, een beschrijving van de categorieën van betrokkenen en die van persoonsgegevens en categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt en eventueel doorgifte van persoonsgegevens aan een derde land. Ten slotte bevat het register, indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens worden gewist en een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die het beveiligingsniveau waarborgen (art. 32). Een verwerker is overeenkomstig lid 2 tevens verplicht een register bij te houden met daarin de naam en contactgegevens van een eventueel aangewezen FG en van iedere vvv voor rekening waarvan de verwerker handelt, de categorieën van verwerkingen die zijn uitgevoerd, eventuele doorgiften en, indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die het beveiligingsniveau waarborgen.

Het bijhouden van een register door een vvv of verwerking kent een uitzondering voor ondernemingen of organisaties die *minder dan 250 personen* in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten *een risico inhoudt* voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of de verwerking bijzondere gegevens of strafrechtelijke gegevens betreft.

Medewerking aan toezichthoudende autoriteit (art. 31 AVG): de vvv en de verwerker werken desgevraagd samen met de toezichthoudende autoriteit bij vervulling van haar taken.

§ 3.6 Persoonsgegevensbeveiliging

De beveiliging van persoonsgegevens is reeds een aantal maal aan bod gekomen. In aansluiting daarop zijn hier regels over vastgelegd in art. 32 t/m 34 AVG. Art. 32 bepaalt allereerst dat de vvv en verwerker *passende technische en organisatorische maatregelen* moeten treffen om een op het risico voor de rechten van een betrokkene afgestemd beveiligingsniveau te waarborgen. Deze maatregelen moeten, waar passend, een aantal aspecten bevatten. Bij deze verplichting moet rekening worden gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, omvang, verwerkingsdoelen en qua waarschijnlijkheid en ernst de uiteenlopende risico's voor de rechten van personen. Voorbeelden van dergelijke maatregelen zijn de pseudonimisering en versleuteling van

⁶³ Kamerstukken II 1997/98, 25892, 3, p. 61 – 62.

persoonsgegevens en een procedure voor het regelmatig testen van de doeltreffendheid van de genomen maatregelen.

Pseudonimisering houdt in dat de verwerking van persoonsgegevens op zodanige wijze gebeurt dat de persoonsgegevens in kwestie niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, eventueel door deze aanvullende gegevens apart te bewaren en maatregelen te treffen dat de betreffende gegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. Hierbij worden identificerende gegevens vervangen door gecodeerde (versleutelde) gegevens. Dergelijk gegevens heten ook wel 'pseudoniemen' en worden samengevoegd in een zogeheten 'dataset'. Pseudonimisering is een goede manier om oppervlakkige, indirecte persoonsgegevens te verzamelen zonder dat deze in verband hoeven te staan met een specifiek persoon. Hier wordt vaak gebruik van gemaakt bij gegevensverwerking met statistische doeleinden. Ook al zijn deze gegevens moeilijk herleidbaar naar een individueel persoon, worden deze als persoonsgegevens gezien. Derhalve is bij dergelijke verwerkingen tevens een wettelijke grondslag, zoals de toestemming van de betrokkene vereist. Onlangs gaf minister Schippers (VWS) kritiek op GGZ-instellingen die zonder toestemming ROM-data (metadata gericht op ervaringen, meningen en/of gevoelens) deelden met een databank.⁶⁴ Binnenkort vindt er door deze verwerkingen tevens een kort geding plaats tegen deze GGZ-instellingen. Wanneer de directe gegevens vernietigd worden, is er echter sprake van anonieme gegevens. Deze gegevens vallen vanwege de niet-herleidbaarheid buiten de reikwijdte van de AVG.

Andere mogelijke maatregelen zijn het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen en het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen. Een laatste voorbeeld van een maatregel is volgens art. 32 lid 1 sub d een procedure handhaven voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking. Bij de beoordeling van het passende beveiligingsniveau wordt volgens lid 2 met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

In art. 33 en 34 AVG is de inhoud van de Wet meldplicht datalekken terug te vinden. Art. 33 richt zich op de melding van een inbreuk in verband met persoonsgegevens (ook wel: datalek) aan de toezichthoudende autoriteit. Deze dient de vzw zonder onredelijke vertraging en, indien mogelijk, uiterlijk binnen 72 uur nadat hij kennis heeft genomen van het datalek te melden bij de bevoegde toezichthoudende autoriteit. Dit hoeft alleen niet te gebeuren wanneer het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten van een natuurlijk persoon. Anders gezegd, het uitgangspunt is melding, tenzij er sprake is van geen of een klein risico. Indien de melding niet binnen 72 uur plaatsvindt, dient de vertraging tezamen met de alsnog gedane melding gemotiveerd te worden. De melding bevat in ieder geval de aard van de inbreuk, het aantal betrokkenen in kwestie, de naam en contactgegevens van FG indien deze is aangewezen, de waarschijnlijke gevolgen van de inbreuk en de maatregelen die de vzw heeft voorgesteld of genomen om het datalek aan te pakken dan wel in te perken. De vzw moet een overzicht bijhouden van alle datalekken.

Art. 35 heeft betrekking op een onverwijld mededeling aan de betrokkene wanneer de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten van een natuurlijk persoon. Deze mededeling bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk en ten minste dezelfde gegevens en maatregelen als de melding aan de autoriteit, zoals in de vorige alinea besproken. De mededeling aan betrokkene is niet vereist

⁶⁴ Oostrom, *Trouw* 19 mei 2017.

wanneer de vvv passende technische en organisatorische beschermingsmaatregelen heeft genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling. Een andere uitzondering op de mededeling is wanneer de vvv achteraf maatregelen heeft genomen om ervoor te zorgen dat het hoge risico niet meer zal voordoen. Ten slotte kan worden volstaan met een openbare mededeling wanneer een persoonlijke mededeling aan betrokkene onevenredige inspanningen zou vergen.

§ 3.7 Privacy Impact Assessment en voorafgaande raadpleging

In art. 35 jo. 36 AVG worden nadere regels over de gegevensbeschermingseffectbeoordeling (ook wel: Privacy Impact Assessment; PIA) en voorafgaande raadpleging beschreven. Dit zijn voorbeelden van nieuwe procedures die, zoals besproken in § 2.3, de meldplicht uit de Wbp vervangen en tegelijkertijd de rechten van betrokkenen dienen te beschermen.⁶⁵

§ 3.7.1 Privacy Impact Assessment (PIA)

Een vvv is volgens art. 35 lid 1 en overw. 91 verplicht om bij verwerkingen die *waarschijnlijk een hoog risico inhouden* voor de rechten van natuurlijke personen, vóór de verwerking een beoordeling uit te voeren van het *effect* van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens in kwestie. Dit dient in het bijzonder te gebeuren wanneer er bij een verwerking nieuwe technologieën worden gebruikt die gelet op de aard, de omvang, de context en de doeleinden daarvan een hoog risico met zich meebrengen. Eén beoordeling kan hierbij een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden. Hierbij moet het advies van een eventueel aangewezen FG worden ingewonnen. Een dergelijke beoordeling is met name nodig bij een systematische en uitgebreide beoordeling (1) van persoonlijke aspecten van natuurlijke personen (2), die is gebaseerd op geautomatiseerde verwerking, waaronder profilering (3), en waarop besluiten worden gebaseerd (4) waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die hem op vergelijkbare wijze wezenlijk treffen (5). Ook wordt een PIA aangeraden bij grootschalige verwerking van bijzondere persoonsgegevens (art. 9) of van strafrechtelijke gegevens (art. 10) en bij grootschalige monitoring van openbaar toegankelijke ruimten. Wat het criterium *hoog risico* behoudens bovenstaande richtlijnen precies inhoudt, zal nog moeten blijken uit bijvoorbeeld jurisprudentie. De beoordeling bevat volgens lid 7 ten minste:

- a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
- b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- c) een beoordeling van risico's voor de rechten van betrokkenen; en
- d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de AVG is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

§ 3.7.2 Voorafgaande raadpleging

Wanneer uit een PIA volgens art. 35 blijkt dat de verwerking een hoog risico zou opleveren indien de vvv geen maatregelen neemt om het risico te beperken, is de vvv op grond van art. 36 lid 1 en overw. 94 verplicht voorafgaand aan de verwerking de toezichthoudende autoriteit te raadplegen. Wanneer deze van oordeel is dat de voorgenomen verwerking inbreuk zou maken op de AVG, geeft de toezichthoudende autoriteit binnen een termijn van acht weken na ontvangst van het verzoek om raadpleging schriftelijk advies aan de vvv en

⁶⁵ Zie ook overw. 89 Preambule AVG.

oefent zij zo nodig een van de haar toegekomen bevoegdheden uit (zie § 3.9.1). Een verzoek tot raadpleging dient in ieder geval informatie te bevatten over de verantwoordelijkheden van de vvv en betrokken verwerkers, de doeleinden en middelen van de voorgenomen verwerking, de maatregelen en waarborgen die worden geboden, de contactgegevens van de FG indien die aangewezen is, de PIA op basis waarvan de raadpleging plaatsvindt en alle andere informatie waar de autoriteit om verzoekt.

§ 3.8 Functionaris voor gegevensbescherming

In sommige gevallen dient er binnen een organisatie een *functionaris voor gegevensbescherming* (FG) aan te worden gewezen. Lid 1 stelt dat een vvv en verwerker in ieder geval een FG moeten aanwijzen wanneer:

- a) de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken; of
- b) een vvv of verwerker hoofdzakelijk is belast met dan wel als hoofdtak heeft verwerkingen uit te voeren die vanwege hun aard, hun omvang en/of hun doeleinden *regelmatige en stelselmatige observatie op grote schaal* van betrokkenen vereisen (bijvoorbeeld een recherchebureau of Google Analytics);⁶⁶ of
- c) de vvv of de verwerker hoofdzakelijk is belast met *grootschalige verwerking van bijzondere categorieën van gegevens* (art. 6) en van persoonsgegevens met betrekking tot *strafrechtelijke veroordelingen en strafbare feiten* (art. 10 lid 2).

De FG wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in art. 39 bedoelde taken te vervullen. De FG kan bovendien een personeelslid van de vvv of de verwerker zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten. Hoe dan ook is het volgens overw. 97 Preambule van belang dat een FG zijn taken en verplichtingen onafhankelijk verricht. Na aanstelling van een FG maakt de vvv of verwerker de contactgegevens van de FG bekend en deelt deze mee aan de toezichthoudende autoriteit. De FG heeft op grond van art. 39 een aantal taken, waaronder in ieder geval het informeren en adviseren van de vvv en werknemers die gegevens verwerken. Denk hierbij aan informatie en adviezen over hun verplichtingen. Ook ziet de FG toe op naleving van de AVG en op het gegevensverwerkingsbeleid van de vvv. Tot dit takenpakket behoort tevens desgevraagd advies verstrekken met betrekking tot PIA's en de uitvoering daarvan, zoals besproken in § 3.7. Ten slotte dient de FG samen te werken met en op te treden als contactpunt voor de toezichthoudende autoriteit.

§ 3.9 Autoriteit Persoonsgegevens en sanctiebevoegdheid

§ 3.9.1 Taken en bevoegdheden

In iedere lidstaat dient overeenkomstig art. 54 AVG een nationale toezichthouder te worden opgericht. In Nederland is dit sinds 1 januari 2016 de Autoriteit Persoonsgegevens (AP, voorheen: CBP). Voornoemd artikel stelt dat het aan iedere lidstaat is om bij wet een aantal zaken omtrent de oprichting, inrichting en takenvaststelling te regelen. Dit wordt in Nederland gedaan in art. 14 – 21 van de voorlopige UAVG. Niettemin worden door de AVG zelf een aantal taken en bevoegdheden opgedragen en toegekend aan de AP die zij dan ook dient uit te voeren (art. 57 en 58 AVG). De belangrijkste taak is het monitoren en handhaven van de toepassing van de AVG, in het bijzonder met betrekking tot de rechten van betrokkenen. Een andere belangrijke taak is de afhandeling van klachten van betrokkenen. Verder is de AP bevoegd een vvv alle voor de uitvoering van haar taken vereiste informatie te verstrekken en om corrigerende maatregelen te nemen zoals door een vvv te berispen met betrekking tot

⁶⁶ Zie ook overw. 97 Preambule AVG

een inbreuk op grond van de AVG. De AP is bovendien bevoegd vww te verplichten een verzoek van een betrokkene in te willigen en bevoegd om toegang te krijgen tot alle noodzakelijke persoonsgegevens en de bedrijfsruimten van een vww. De bepalingen in de UAVG zien vooral toe op de specifieke inrichting van de AP.

Iedere betrokkene binnen de EU heeft, onverminderd andere juridische mogelijkheden zoals het instellen van beroep bij de rechter of het starten van een civiele procedure wegens een onrechtmatige daad, het recht een klacht in te dienen bij de toezichthoudende autoriteit. Ook hebben zij volgens art. 82 AVG recht op een schadevergoeding van een vww of verwerker voor geleden (im)materiële schade. Elke vww die bij de verwerking is betrokken, is aansprakelijk voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op de AVG. Een vww of verwerker is echter niet aansprakelijk indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

§ 3.9.2 Sanctiebevoegdheid

Nationale toezichthouders zijn op grond van de AVG tevens bevoegd sancties op te leggen aan vww's en verwerkers, zoals in de vorm van *administratieve geldboetes*. Deze moeten volgens art. 83 doeltreffend, evenredig en afschrikwekkend zijn en kunnen worden opgelegd naast of in plaats van de andere maatregelen die openstaan voor de nationale toezichthouder. Deze maatregelen zijn opgesomd in art. 58 en hiervan zijn er in subparagraaf 1 reeds een aantal besproken. Art. 84 AVG geeft lidstaten de ruimte om andere sancties vast te stellen, in het bijzonder die geen administratieve boete tot gevolg hebben. Een voorbeeld hiervan is art. 17 in de voorlopige UAVG die de AP mogelijkheid biedt om een last onder bestuursdwang op te leggen op basis van art. 83 AVG. De voorlopige UAVG vult deze mogelijkheid aan door opvallend genoeg te stellen dat een administratieve boete in dat geval niet noodzakelijk is, omdat de praktijk zou uitwijzen dat de last onder bestuursdwang en dwangsom effectieve middelen zijn om overtredingen op de regels inzake bescherming van persoonsgegevens snel te beëindigen.

In lid 2 van art. 83 AVG wordt een groot aantal factoren behandeld die meespelen bij de bepaling van de hoogte van een boete. Factoren zijn onder andere de aard, ernst en duur van de inbreuk. Daarnaast moet worden gekeken naar de maatregelen die zijn genomen om de inbreuk te voorkomen, te verhelpen dan wel te beperken. Ook is relevant op welke categorieën van persoonsgegevens de inbreuk betrekking heeft en in hoeverre er sprake is van opzet of nalatigheid door de vww. In lid 4 en 5 van art. 83 worden vervolgens twee categorieën met inbreuken en daaraan gekoppelde boetes onderscheiden:

1. Geldboetes tot € 10.000.000,- of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is dan dat bedrag. Hieronder vallen onder andere de inbreuken op de verplichtingen van de vww en de verwerker overeenkomstig de artikelen 8 (toestemming kinderen), 11 (betrokkene op de hoogte stellen dat hij niet te identificeren is), 25 tot en met 39 (verplichtingen vww, inclusief datalekken) en 42 en 43 (certificering).
2. Geldboetes tot € 20.000.000,- of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is dan dat bedrag. Hieronder vallen onder andere de inbreuken op basisbeginselen inzake verwerking, met inbegrip van de voorwaarden voor toestemming (art. 5, 6, 7 en 9), de rechten van betrokkenen volgens art. 12 t/m 22, de doorgifte van persoonsgegevens aan een ontvanger in een derde land (art. 44 t/m 49) en alle verplichtingen genoemd in hoofdstuk IX (Bepalingen in verband met specifieke situaties).

De voorlopige UAVG bepaalt verder in art. 14 lid 3 dat in het Nederlands recht onder 'administratieve geldboete' wordt verstaan: een bestuurlijke boete. Ook wordt in art. 18 de bevoegdheid toegekend om een boete uit de tweede categorie op te leggen indien een inbreuk wordt gepleegd op het verbod tot verwerking van strafrechtelijke gegevens.

Hoofdstuk 4 Praktijksituatie VM-Concepts

In dit hoofdstuk wordt de gewenste praktijksituatie rondom VM-Concepts, Vraagmaatje en de verwerking van persoonsgegevens uitgebreid beschreven. Deze voornemens zijn enerzijds onderzocht door middel van interviews met de initiatiefnemers van Vraagmaatje, ook wel bestuurders van VMC. Het gaat om de heer Van den Boom, de heer Meulendijks en de heer Van Rooy. De geautoriseerde uitwerkingen van deze interviews zijn aan dit rapport toegevoegd als bijlagen I t/m III. Daarbij is tevens nuttige informatie gehaald uit de PowerPointpresentaties die VMC heeft gehouden voor haar doelgroep (de leden van KBO-Brabant). Anderzijds is door het houden van een enquête bij tien bij Vraagmaatje betrokken KBO-leden nagegaan in hoeverre zij als gebruikers bezwaar hebben tegen het gebruik van hun persoonsgegevens. Dit heeft betrekking op de ethische aspecten die aan bod komen in § 6. Deze enquête is opgenomen als bijlage IV van dit onderzoeksrapport.

§ 4.1 VM-Concepts

VM-Concepts (VMC) is een startup met de gedachte van een social enterprise. Dit betekent dat geld verdienen niet het hoofddoel is, maar geld wel een middel is om bij te kunnen dragen aan de maatschappij. Kenmerkend voor een startup is dat er naar een ideaal beeld wordt toegewerkt en dat er gaandeweg nog veel aanpassingen gedaan worden. Dit betekent ook dat er in de startupfase nog veel onduidelijk is en er meer wordt gedacht in mogelijkheden in plaats van onmogelijkheden. Wel is duidelijk dat VMC een bv i.o. (in oprichting) is met in totaal drie bv's en een vof als aandeelhouders. Dit zijn: The Legal Network Office vof (ook wel: Advocabo), Mimese bv, Het Gulden Vlies Holding bv en Harvest Social Enterprise bv. Zij zullen voor gelijke delen aandeelhouder zijn in VMC. Capgemini Group Nederland⁶⁷ is een van de samenwerkingspartners. De bedoeling is dat zij samen met Harvest het prototype van het platform 'Vraagmaatje' en de verdere digitale omgeving zal ontwikkelen en beheren. VMC richt haar bedrijfsvoering voorlopig nog op Nederland en staat voorlopig ingeschreven op het kantoor van een van de bestuurders in Sint-Michielsgestel. Afhankelijk van de resultaten, zou er volgens VMC in een later stadium een geheel eigen kantoor kunnen worden gekozen. De primaire doelgroep zijn ouderen, met name die lid zijn van KBO-Brabant. KBO-Brabant is een belangenbehartigingsorganisatie voor senioren.⁶⁸

§ 4.2 Vraagmaatje

Vraagmaatje is het te ontwikkelen platform en de reden waarom dit privacyonderzoek is ingesteld. Volgens de initiatiefnemers moet Vraagmaatje worden gezien als een 'digitale buddy' (een helpdesk; vraagbaak) in de vorm van een portaal⁶⁹ die directe toegang biedt tot allerlei applicaties (toepassingen) die gebruikmaken van nieuwe technologieën, waaronder kunstmatige intelligentie. Dit is de intelligentie waarmee zelflerende machines, software en apparaten zelfstandig problemen oplossen, waarbij deze het denkvermogen van een mens imiteren.⁷⁰ Het portaal overkoepelt als het ware die applicaties. Toegang tot Vraagmaatje kan worden verkregen met een vingerafdruk, of door stem- of gezichtsherkenning. Na de verkregen toegang kan een gebruiker de applicaties gebruiken. Een van die toepassingen maakt het mogelijk voor een gebruiker om zelf te vragen om ondersteuning. Een voorbeeld hiervan is het verzoek tot het opstellen van een offerte voor een hypotheek of een verzoek van de gebruiker om hem in contact te brengen met een bepaalde hypotheekaanbieder. Ook zou er een applicatie kunnen komen die door gebruikers gemaakte foto's van zakelijke documenten kan analyseren en beoordelen. Nog een voorbeeld van een applicatie binnen Vraagmaatje is een webbrowser die het mogelijk maakt om anoniem te surfen (zie § 5).

⁶⁷ nl.capgemini.com

⁶⁸ kbo-brabant.nl

⁶⁹ Een poortal (portal) is een online omgeving die toegang geeft tot verschillende websites of applicaties.

⁷⁰ Kunstmatige intelligentie, [Mediawijsheid.nl](http://mediawijsheid.nl).

Een andere, belangrijke toepassing zal een persoonlijke mailbox met een eigen, weliswaar door VMC aangemaakt, e-mailadres zijn. In deze mailbox kunnen belangrijke mails van allerlei organisaties, inclusief aanverwante stukken, naar de gebruiker toe worden gestuurd. Een applicatie binnen Vraagmaatje zal deze mails en stukken analyseren, aangeven wat de betekenis is van de inhoud, deze beoordelen en zal vervolgens adviseren over wat er vervolgens mee moet gebeuren. De mailbox maakt het tevens mogelijk om mails vanuit datzelfde e-mailadres terug te sturen naar de betreffende organisatie.

Hoe?

Concreet kan dit betekenen dat er een mail binnenkomt van bijvoorbeeld: de gemeente met een WOZ-beschikking, een energieleverancier met de jaarafrekening, een werkgever met een loonstrook, een woningcorporatie met een huurfactuur, een uitkeringsinstantie met een besluit, een zorgverzekeraar met een polis, banken met berichten over internetbankieren, of een telecombedrijf met een telefoonrekening of -abonnement. Indien de inhoud van een mail met bijgevoegd document onjuist blijkt, zal Vraagmaatje naast preventief ondersteunen en adviseren, waar mogelijk proberen een actieve rol te spelen bij de oplossing van het geschil. Een voorbeeld van ondersteuning is het in contact brengen van een gebruiker met de betreffende organisatie. De bedoeling hierbij is dat Vraagmaatje alle nodige gegevens toont aan de gebruiker zelf en de vraag van de gebruiker helder voor hem formuleert, zodat deze voorbereid het gesprek in kan gaan.

Het is niet de bedoeling dat Vraagmaatje direct zaken regelt met de andere partij, zoals het regelen van een betaling voor een gebruiker. Het zal wel aangeven of, hoe en wanneer dit moet gebeuren. Daarnaast is gewenst dat Vraagmaatje voor een gebruiker een document kan opstellen, zoals een bezwaar tegen de beschikking van een gemeente. Alle bovenstaande zaken hebben gemeen dat zij door de gebruiker als complex kunnen worden ervaren en dat deze een formeel karakter hebben. Vraagmaatje is dus niet bedoeld om te weten te komen hoe lang de langste mens ooit was. Voor de nieuwsgierigen onder ons, het antwoord is 272 cm lang.

Vraagmaatje zal op een toegankelijke, menselijke manier via spraak en beeld te gebruiken zijn. Met 'beeld' wordt bedoeld dat Vraagmaatje wordt weergegeven als een geanimeerd persoon. De bedoeling is dat Vraagmaatje een echt gesprek aangaat met een gebruiker. Ook is het de bedoeling dat Vraagmaatje kennis en informatie van en over gebruikers opslaat en vervolgens handelt vanuit deze kennis. Vraagmaatje zal zaken daardoor sneller en beter kunnen interpreteren. Hierdoor zal Vraagmaatje zelfstandig en autodidact zijn en zullen gebruikers steeds beter en gemakkelijker geholpen kunnen worden. In het begin zal er nog veel menselijke ondersteuning zijn. Zo zal een gebruiker op het moment dat deze niet binnen een aantal minuten goed is geholpen door het systeem van Vraagmaatje, worden doorgeschakeld naar een helpdeskmedewerker. Vraagmaatje moet in dat kader dus worden gezien als eerstelijns ondersteuning. Verder zal het voor de gebruiker mogelijk zijn om bijvoorbeeld familieleden, mantelzorgers of instanties toestemming te geven om mee te kijken in het systeem en deze zo te ondersteunen.

Waarom?

Het achterliggende doel is om de gebruiker te ontzorgen door deze bij allerlei formele zaken te ondersteunen en daar waar mogelijk (juridische) conflicten vroegtijdig te voorkomen. Dit zijn veelal zaken die door gebruikers, met name ouderen, als complex worden ervaren. Wanneer de situatie toch tot een conflict leidt, wil Vraagmaatje deze oplossen of aangeven hoe de gebruiker deze kan oplossen. Hierbij zou Vraagmaatje kunnen doorverwijzen naar andere organisaties, zoals naar Advocabo voor de juiste juridische bijstand.

§ 4.3 Financiële aspecten

Om het principe van de social enterprise uit te kunnen voeren en gebruikers zo goed mogelijk van dienst te kunnen blijven, heeft VMC de middelen hiervoor nodig. Deze middelen

wil zij genereren met behulp van een aantal bronnen van inkomsten die tevens zijn uitgewerkt in een verdiemodel. Het gaat om de volgende bronnen van inkomsten:

- Vraagmaatje zal worden aangeboden aan gebruikers die hiervoor direct een vast (maandelijks) bedrag betalen, of zal worden aangeboden bij het aangaan van een lidmaatschap met KBO-Brabant, net als Spotify bij KPN wordt aangeleverd. Indien KBO-Brabant hiervoor openstaat, zullen KBO-leden lidmaatschapsgeld betalen aan KBO en zal KBO een deel hiervan afstaan aan VMC voor het gebruik van Vraagmaatje.
- VMC twijfelt nog over (gedeeltelijke) betaling met persoonsgegevens. Dit zou betekenen dat naast een vast tarief een gereduceerd tarief aan wordt geboden op het moment dat een gebruiker meer gegevens ter beschikking stelt.
- Bovendien wil VMC contracten sluiten met grote bedrijven en met instanties (contractspartijen) die tegen betaling metadata aangeleverd krijgen. Die metadata zorgt voor waardevolle informatie waarmee zij hun dienstverleningen zoals hun klantenservices optimaliseren. De contractspartijen hebben volgens VMC tevens baat bij een samenwerking met VMC, omdat een deel van de communicatie tussen die organisaties en haar klanten via Vraagmaatje verloopt. VMC vermoedt dat die organisaties zo kunnen besparen op hun klantenservices.
- Voor VMC is een andere mogelijkheid om op het moment dat Vraagmaatje verder gevorderd is, om de technologie die is gebruikt voor Vraagmaatje aan te bieden aan andere bedrijven. Die zouden deze technologie bijvoorbeeld kunnen gebruiken ter vervanging van een medewerker van de klantenservice.
- Een mogelijkheid voor de latere termijn is om met kunstmatige intelligentie een omgeving te vormen waarin geld wordt verdiend aan Big Data in combinatie met algoritmes.
- VMC wil in ieder geval geen persoonlijke gegevens vrijgeven aan derden, of persoonlijke advertenties aanbieden wanneer een gebruiker hier niet om heeft gevraagd. Wel wil zij wellicht de gebruiker een optie geven te verzoeken om persoonlijke advertenties over een bepaald onderwerp. In dat geval zouden bedrijven VMC kunnen betalen om via Vraagmaatje te adverteren aan deze gebruikers.

§ 4.4 Verwerking van persoonsgegevens

VMC wil zo veel mogelijk gegevens van Vraagmaatje-gebruikers verwerken, waaronder directe persoonsgegevens zoals naam, adres, woonplaats, geslacht, leeftijd, geboortedatum en telefoonnummer. Daarnaast wil VMC beschikken over alle gegevens over het dagelijkse leven van gebruikers, zolang deze een formeel karakter bezitten. Bij een formeel karakter dient te worden gedacht aan financiën, gezondheid, zorg, administratie et cetera. Hierbij horen ook de bankrekeninggegevens en pincodes van een gebruiker en de klantnummers en polisnummers van een gebruiker bij een bepaalde organisatie. Bovendien is de wens om biometrische gegevens van gebruikers vast te leggen, zodat de gebruiker deze kan gebruiken om toegang te krijgen tot Vraagmaatje. Dit kan door middel van een vingerafdruk, irisscan of gezichts- of stemherkenning. Ook wil VMC de wachtwoorden die de gebruiker heeft bij de applicaties binnen Vraagmaatje tot hun beschikking hebben en deze beheren (zie § 5). Doordat Vraagmaatje deze gegevens bewaart, zijn de applicaties door in te loggen bij Vraagmaatje direct toegankelijk voor de gebruiker. Met alle bovenstaande gegevens wil VMC bereiken dat Vraagmaatje de gebruiker zo goed mogelijk leert kennen en hem steeds beter en sneller kan helpen met steeds meer vraagstukken. De gegevens kunnen niet alleen worden ingezet voor de applicatie met de inkomende mails, maar ook voor de applicaties waar de gebruiker zelf kan vragen om ondersteuning.

Verder wil VMC metadata (generieke gedragsgegevens) vormen uit gegevens die gebruikers ter beschikking stellen; hun input. Er kan zich bijvoorbeeld een situatie voordoen waarin meerdere gebruikers een vraag stellen over een bepaald onderwerp of klagen over een bepaalde situatie. Stel: in een bepaalde periode klagen meer gebruikers over hun maandfactuur bij Ziggo dan normaal en volgens de beoordeling van de applicatie blijkt de factuur niet te kloppen. Of in een bepaalde periode moet de gemiddelde gebruiker vijftien minuten wachten voordat hij werd geholpen door de klantenservice. Dit geeft de ervaringen van gebruikers met een contractspartij weer. Het is in die situaties voor VMC niet relevant wie precies de vraag heeft gesteld of heeft geklaagd, waardoor hier metadata van te vormen is. Hierbij wordt informatie gebruikt van meerdere gebruikers (groepen), waardoor deze zo onpersoonlijk mogelijk zijn. Deze informatie kan vervolgens op gestandaardiseerde wijze worden aangeleverd aan een contractspartij, onder andere in de vorm van feedback of een klantenbeoordeling. Hierdoor worden de prestaties van de betreffende contractspartij meetbaar. Voor de contractspartij iijkt dit volgens VMC interessante informatie.

§ 4.5 Voorgenomen beveiliging

VMC heeft een aantal plannen opgesteld met betrekking tot de beveiliging van de persoonsgegevens van en over gebruikers. Zo zullen alle persoonsgegevens worden opgeborgen in een digitale, beveiligde '(privacy)kluis'. Deze gegevens zijn enkel toegankelijk voor de gebruiker zelf en voor VMC om gebruikers te kunnen helpen met hun vragen en problemen. In deze 'kluis' zijn ter beveiliging tevens de wachtwoorden van de toepassingen binnen Vraagmaatje opgeslagen. Wanneer deze zijn verlopen zal VMC deze ook opnieuw instellen, zodat deze niet gemakkelijk te kraken zijn door hackers. Zoals gezegd kan de kluis alleen worden geopend met de biometrische gegevens van een gebruiker. VMC heeft geen andere plannen met de gevoelige gegevens zoals de wachtwoorden die zich in deze kluis bevinden. Deze privacykluis is volgens VMC alleen bedoeld ten dienste van de gebruiker.

Bovendien is er het voornemen om de anonimiteit van gebruikers naar de buitenwereld toe te waarborgen, zodat zij Vraagmaatje op een veilige en vertrouwde manier kunnen gebruiken. Normaal gesproken wordt een computer automatisch verbonden met een andere computer op het moment dat iemand het internet betreedt. Daarbij komen, vaak met behulp van cookies⁷¹, veel gegevens over die persoon vrij voor de betreffende website of applicatie. Door het instellen van een (anonieme) proxyserver⁷² wordt de computer eerst verbonden met de proxyserver als tussenpersoon. Deze proxyserver zou kunnen worden geplaatst bij VMC zelf. Het verkeer tussen computers verloopt dan via de proxy. Hierdoor blijven gegevens van die persoon, waaronder het oorspronkelijke IP-adres, anoniem voor derden. Een proxyserver komt met name van pas bij de browserapplicatie binnen Vraagmaatje. VMC wil iedere gebruiker verbinden met dezelfde proxyserver, zodat zij allen vanaf één plek veilig kunnen surfen. Zij zijn daardoor niet identificeerbaar (herleidbaar).

Ten slotte is VMC van plan een onafhankelijke toezichthouder aan te stellen die controleert of VMC zich aan de privacyregels van de AVG houdt. Zo zal deze blijven toetsen of gehoor wordt gegeven aan de rechten van gebruikers en of VMC voldoende transparant is naar haar gebruikers toe. VMC heeft aangegeven dat hiervoor een rol kan zijn weggelegd voor KBO-Brabant, of dat het wellicht mogelijk is een stichting op te richten met een raad van toezicht.

§ 4.6 Ethische aspecten

Buiten de juridische vereisten is het bij een onderwerp als privacy verstandig om te oordelen of een gewenste handelwijze moreel gezien wel gepast is. Het is immers essentieel om een

⁷¹ Een cookie is een databestand datp een computer worden achtergelaten nadat een website is bezocht. Hierdoor kunnen bedrijven onder andere iemands surfgedrag en locatie achterhalen en met behulp hiervan persoonlijke advertenties aanbieden. Klous & Wielaard 2016, p. 22.

⁷² 'Proxy' betekent in het Engels ook wel '*one appointed or authorized to act for another*'. In het Nederlands komt dit neer op 'een gevolmachtigd tussenpersoon'.

vertrouwensband te hebben met de klant (hier: gebruiker van Vraagmaatje). Een gebrek aan vertrouwen kan voortkomen uit onvoldoende informatie en/of transparantie en kan weerstand oproepen bij gebruikers.⁷³ Recente onderzoeken versterken dit beeld, zoals een onderzoek onder 24.143 internetgebruikers uit 24 landen waaruit bleek dat 79% van de ondervraagden zich zorgen maakt over het gebrek aan online privacy.⁷⁴ In het kader van dit rapport is een enquête gehouden onder tien KBO-leden die reeds zijn betrokken bij workshops over Vraagmaatje. In deze enquête zijn vragen gesteld over in hoeverre potentiële gebruikers bezwaar hebben tegen het gebruik van hun persoonsgegevens. Er is ten eerste gevraagd wat zij ervan zouden vinden als hun gegevens voor interne dan wel externe doeleinden zouden worden verwerkt. Vervolgens is gevraagd in hoeverre hun antwoorden afhankelijk zijn van de soort gegevens, de transparantie en het al dan niet gratis gebruik.

- Drie respondenten geven aan het geen probleem te vinden wanneer zijn persoonsgegevens inzichtelijk zijn voor Vraagmaatje. Zes van hen geeft aan Vraagmaatje liever te gebruiken zonder dat deze inzichtelijk zijn. Eén KBO-lid geeft aan dat dit afhangt van welke persoonsgegevens voor welke doeleinden en onder welke voorwaarden worden verwerkt.
- Zeven respondenten geven aan weinig bezwaar te hebben tegen het feit dat zijn gegevens enkel inzichtelijk zouden zijn voor Vraagmaatje doordat deze voor een bepaalde periode worden opgeslagen. (twee – drie sterren). Drie mensen zeggen dit toch wel bezwaarlijk te vinden (vijf sterren).
- Acht direct betrokkenen zijn van mening geen tot weinig problemen in te zien van de verwerking van zijn gegevens met als doel dat Vraagmaatje deze gebruikt om de gebruiker zo goed mogelijk van dienst te kunnen zijn (één – drie sterren). Twee anderen geven aan hier wel bezwaar tegen te hebben (zes sterren).
- De antwoorden op de vraag of hun gegevens mochten worden gebruikt om de werkwijze van Vraagmaatje te optimaliseren en zo ook andere gebruikers beter van dienst te kunnen zijn, waren verschillend. Vier gaven aan geen enkel bezwaar te hebben (één ster), twee mensen hebben (een beetje) bezwaar (twee – vier sterren) en drie respondenten hebben bezwaar tegen deze situatie (vijf – zes sterren). Voor één persoon zou het een reden zijn om Vraagmaatje niet te gebruiken (zeven sterren.)
- Drie respondenten maken duidelijk er geen probleem mee te hebben indien VMC metadata vormt uit haar gegevens die kan worden gedeeld met organisaties die daarmee hun dienstverleningen kunnen verbeteren. Drie mensen hebben lichte bezwaren (drie sterren), twee mensen hebben grotere bezwaren (vijf – zes sterren) en twee KBO-leden geven aan Vraagmaatje om deze reden niet te willen gebruiken (zeven sterren).
- Uit de vraag of het verschil maakt om welke gegevens het hierbij gaat, geven de KBO-leden over het algemeen aan minder bezwaar te hebben met direct persoonsgegevens zoals naw-gegevens en leeftijd. Voor hen zijn gegevens over geloof, gezondheid en politieke opvattingen echter te persoonlijk om te delen. Daarnaast geven de KBO-leden aan dat naarmate de manier waarop hun gegevens worden gebruikt duidelijker en inzichtelijker is, de kans groter is dat zij Vraagmaatje gebruiken. Wanneer dit onvoldoende gebeurt willen zij Vraagmaatje niet gebruiken. Ten slotte maakt het voor hen weinig verschil of de dienst gratis is of niet.

Kortom, over het algemeen is het vertrouwen in Vraagmaatje goed. Wel lijkt het voor de respondenten belangrijk om welke gegevens het gaat en hoe transparant VMC is.

⁷³ Martijn 2016, p. 45.

⁷⁴ Centre for International Governance Innovation & Ipsos 2016 en Klous & Wielaard 2016, p. 12.

Hoofdstuk 5 Conclusies en aanbevelingen

Dit slothoofdstuk richt zich allereerst op het opstellen van conclusies door de privacyregels van de AVG te koppelen aan de gewenste praktijksituatie. Hiermee wordt antwoord gegeven op de centrale vraag: *“op welke wijze dient VM-Concepts de gewenste verwerking van persoonsgegevens in te richten, zodat deze voldoet aan de Algemene verordening gegevensbescherming?”*. Met andere woorden, door deze conclusies wordt voor VMC helder hoe zij haar verwerkingsproces dient in te richten. Op basis hiervan worden aanbevelingen gedaan in de vorm van enerzijds een checklist met de punten waaraan VMC volgens de AVG moet voldoen, voordat Vraagmaatje wordt aangeboden. Anderzijds is er een stroomdiagram opgesteld dat moet worden gevolgd om stapsgewijs na te gaan hoe de voorgestelde inrichting van de verwerking in de werkprocessen van VMC moet worden geïmplementeerd. Zo voorkomt VMC dat zij in strijd handelt met de AVG en zorgt zij ervoor dat de gegevensbescherming van betrokkenen wordt gewaarborgd.

§ 5.1 Conclusies

Reikwijdte

VMC valt onder de reikwijdte van de AVG, omdat zij voornemens is bedrijfsmatig allerlei categorieën van persoonsgegevens van natuurlijke personen te verwerken binnen de EU. VMC zal hierdoor in eerste instantie bij iedere handeling na moeten gaan of deze door de AVG wordt bestempeld als een verwerking van persoonsgegevens. Hiervan is in dit geval al snel sprake. Vrijwel iedere handeling wordt namelijk gezien als een verwerking en vrijwel alle gewenste verwerkingen door VMC betreffen persoonsgegevens die te herleiden zijn of kunnen worden herleid tot een individuele gebruiker. Ook bij gepseudonomiseerde gegevens zoals bij metadata die VMC wil verwerken is deze kans er, omdat losgekoppelde persoonlijke gegevens zich nog wel in het systeem bevinden. Gebruikers van Vraagmaatje zijn in relatie tot de AVG ‘betrokkenen’. VMC is in dat kader de verwerkingsverantwoordelijke.

Beginselen

VMC dient bij al haar verwerkingen te allen tijde rekening te houden met de beginselen voor gegevensverwerking. Bij het transparantiebeginsel is voor VMC van belang dat zij eerlijk moet zijn over haar werkwijze en de betrokkene op duidelijke en begrijpelijke wijze moet informeren. Dit is onder andere mogelijk door een kort en bondig gegevensverwerkingsbeleid met transparante, begrijpelijke privacyvoorwaarden op te stellen. Door dit beleid dient voor de betrokkene duidelijk te zijn welke persoonsgegevens op welke wijze en met welke doeleinden worden verwerkt. Om een realistisch, handhaafbaar beleid te bewerkstelligen is het van belang dat de voorgenomen verwerkingen evenredig blijven aan de getroffen maatregelen. De mogelijkheid bestaat om te starten met de verwerking van reguliere, niet-bijzondere persoonsgegevens, totdat de maatregelen zijn voorbereid op de verwerking van bijvoorbeeld bijzondere en/of strafrechtelijke gegevens. Een goede aanvulling op deze middelen zou zijn om de kern van het beleid tevens aan de betrokkene uit te leggen in een kort filmpje.

Bij het rechtmatigheidsvereiste geldt dat een grond voor de verwerking, beslist in het geval van bijzondere en strafrechtelijke persoonsgegevens, noodzakelijk (proportioneel) moet zijn. De inbreuk op het belang of recht van een betrokkene mag namelijk niet onevenredig zijn in verhouding tot het doel van die verwerking. De rechtmatigheid zal in het geval van VMC vooral moeten blijken uit de toestemming van een betrokkene. Een aantal gegevens zoals de naam en adresgegevens en het e-mailadres en telefoonnummer van een gebruiker kunnen worden verzameld met de grond dat deze noodzakelijk zijn voor de uitvoering van de overeenkomst. Hieronder vallen bijvoorbeeld de gegevens ten behoeve van het klantenbestand van VMC. Hierbij doet VMC er verstandig aan om bij te houden welke gegevens op welke grond zijn verzameld, of om deze gegevens gescheiden te houden. De toestemming zou kunnen worden gevraagd op het moment dat de gebruiker de software installeert of wanneer geen installatie nodig is, op het moment dat de gebruiker de portal

voor het eerst betreedt. Gezien de vele voorgenomen verwerkingen is het extra belangrijk dat deze toestemming vrij, specifiek, geïnformeerd en ondubbelzinnig plaatsvindt. In plaats van gebruik te maken van een (dubbele) opt-in, kan er ook worden gekozen voor het opstellen en aanbieden van een formulier voor een verklaring van de toestemming. Hierin moet in begrijpelijke en toegankelijke vorm en in duidelijke en eenvoudige taal worden uitgelegd waarvoor de betrokkene toestemming verleent. Deze ingevulde verklaring zou door VMC moeten worden opgeslagen, zodat zij kan aantonen dat deze toestemming is verleend. Daarnaast is VMC verplicht de betrokkene de mogelijkheid te bieden om de gegeven toestemming eenvoudig in te trekken. Ook dit kan worden gedaan door het opstellen en aanbieden van een formulier of door een omgekeerde (dubbele) opt-in. Een belangrijke kanttekening bij de toestemming is dat ook voor het verwerken van metadata toestemming van de betrokkene zal moeten worden gevraagd.

Het beginsel van doelbinding en onverenigbaar gebruik houdt voor VMC concreet in dat voorafgaand aan een verwerking vast moet staan volgens welke welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden bepaalde gegevens worden verwerkt. Een voorbeeld van een omschreven doel kan zijn: “er worden gegevens over uw gezondheid verzameld, zodat u op uw verzoek kan worden geadviseerd over uw zaken met uw zorgverzekeraar”. De betreffende gegevens mogen vervolgens slechts met een ander doel verder worden verwerkt wanneer de betrokkene dit mocht verwachten. Hiervan is in zekere zin sprake doordat een gebruiker zich ervoor leent zijn gegevens beschikbaar te stellen, zodat hij op allerlei manieren kan worden ondersteund. Daardoor is het immers moeilijk te voorkomen dat met dezelfde gegevens verschillende verwerkingen plaatsvinden. De regel blijft echter dat voor iedere nieuwe verwerking met een ander doel dan het oorspronkelijke doel een nieuwe rechtsgrond is vereist.

Verder zal VMC zo kort mogelijke termijnen moeten vaststellen waarbinnen bepaalde (categorieën) gegevens zullen worden gewist. Hierbij kan zij in ieder geval de waarborg stellen dat gegevens worden gewist op het moment dat een betrokkene aangeeft geen gebruik meer te willen maken van Vraagmaatje. Daarnaast is het verstandig om in ieder geval ieder halfjaar een periodieke toetsing van persoonsgegevens te doen. Niet alleen kan worden getoetst of gegevens gewist kunnen worden, maar ook of deze juist of onvolledig zijn waardoor deze moeten worden gerectificeerd dan wel aangevuld.

Bijzondere persoonsgegevens

VMC heeft aangegeven ook veel bijzondere persoonsgegevens te willen verwerken, waaronder gezondheidsgegevens en biometrische gegevens van gebruikers. Doordat de verwerking van deze gegevens in beginsel verboden is, moet VMC nagaan of deze gezien de belangen van de betrokkene wel noodzakelijk zijn. Deze verwerkingen zijn wel toegestaan indien de betrokkene zijn uitdrukkelijke toestemming heeft gegeven. Het is VMC toegestaan om biometrische gegevens te verwerken met het oog op de identificatie van de gebruiker wanneer deze wil inloggen bij Vraagmaatje. Dit is immers tegelijkertijd een passende maatregel ter beveiliging van de persoonsgegevens van een betrokkene en derhalve proportioneel. Strafrechtelijke gegevens zouden kunnen worden verwerkt wanneer dit noodzakelijk is op het moment dat een gebruiker vraagt om een advies in een juridische zaak.

Rechten betrokkenen

VMC moet redelijke maatregelen treffen om zo voldoende rekening te houden met de rechten van betrokkenen. Een betrokkene dient hierbij in staat te worden gesteld om zijn rechten gemakkelijk uit te oefenen, zoals door middelen die het voor hem mogelijk maken om gemakkelijk en kosteloos een verzoek in te dienen. Dit zou mogelijk zijn door een duidelijk, invulbaar formulier (bijvoorbeeld een verzoek tot inzage) op te stellen en aan de betrokkene aan te bieden. Indien een betrokkene een verzoek tot uitoefening van een recht heeft gedaan, mag dit verzoek alleen door VMC worden geweigerd wanneer zij na onderzoek oordeelt dat het verzoek onterecht of onjuist is. Er dient in ieder geval binnen één

maand te worden gereageerd op het verzoek. Verder moet VMC ervoor zorgen dat al haar informatie en communicatie richting de betrokkene transparant, duidelijk, begrijpelijk en eenvoudig toegankelijk is. Dit wil zeggen: geen lange teksten met moeilijke taal, maar concreet en in heldere taal. Als onderdeel van de duidelijke communicatie en informatie moet VMC de betrokkene onverwijld inlichten wanneer zijn persoonsgegevens bij de betrokkene worden verzameld en wanneer deze niet van de betrokkene zijn verkregen.

Verantwoordelijkheden verwerkingsverantwoordelijke en verwerker

De rol van VMC als verwerkingsverantwoordelijke brengt allerlei verplichtingen met zich mee, zoals het vaststellen van de verantwoordelijkheden en de gewenste verwerkingen met de daarbij horende doeleinden en middelen. Aangezien dit nog niet concreet en unaniem is gebeurd, zullen de bestuurders van VMC dit op korte termijn gezamenlijk moeten doen. Daarnaast zal VMC bij de inschakeling van een extern bedrijf dat ten behoeve van Vraagmaatje een verwerking verricht, zoals Capgemini, een verwerkersovereenkomst met die organisatie moeten tekenen. Hierin kunnen afspraken worden vastgelegd over de wijze waarop de verwerker omgaat met persoonsgegevens. Eventuele medewerkers van VMC worden gekwalificeerd als intern beheer. VMC zou deze een geheimhoudingsovereenkomst moeten laten tekenen om hen meer te kunnen vertrouwen met de aanwezige persoonsgegevens.

Hoewel VMC minder dan 250 personen in dienst heeft, is zij verplicht een register van verwerkingsactiviteiten bij te houden. De reden hiervoor is dat zij bijzondere gegevens wil verwerken, verwerkingen wil verrichten die niet incidenteel zijn en omdat het waarschijnlijk is dat de verwerking die zij zal verrichten een risico inhoudt voor de rechten van betrokkenen. Dit register kan zij in een beveiligde digitale omgeving bijhouden met daarin de juridisch vereiste informatie. VMC dient ervoor zorg te dragen dat iedere verwerking in dit register wordt opgeslagen.

Persoonsgegevensbeveiliging

VMC moet passende maatregelen treffen om een op het risico voor de rechten van een betrokkene afgestemd beveiligingsniveau te waarborgen. De informatiesystemen zoals de servers die voor het platform worden gebruikt zullen zowel fysiek als digitaal goed moeten worden beveiligd. Denk bij fysieke maatregelen aan servers bij een datacenter met vergrendelde deuren, toegangscontroles, back-up stroomvoorzieningen, vastlegging van gebruik door back-ups en aan calamiteitenplannen. Digitaal kan dit worden gerealiseerd door de systemen zodanig te laten beveiligen dat deze niet eenvoudig door ongewenste personen te kraken zijn. Dit geldt in het bijzonder voor de voorgestelde mailbox en privacykluis. Deze bevatten zodanig veel (bijzondere) persoonsgegevens van en over een gebruiker, dat deze een hoog risico voor hem inhouden. Hier kan een deskundige voor worden ingeschakeld.

Pseudonimisering kan tevens worden gezien als een geschikte maatregel, omdat oppervlakkige, indirecte gegevens gescheiden worden gehouden van directe persoonsgegevens en worden gevormd tot een abstracte (meta)dataset. Zo is het lastiger om bepaalde gegevens te laten herleiden tot een individueel persoon. Het is ook een mogelijkheid om de directe persoonsgegevens te vernietigen in plaats van apart te bewaren, zodat sprake is van anonimisering. In dat geval vallen de persoonsgegevens buiten de reikwijdte van de AVG. Wel moet hierbij worden opgepast dat door loskoppeling of wissing van persoonsgegevens geen onvolledig beeld van een betrokkene mag ontstaan (dataminimalisatie). Daarnaast is het verstandig om bestanden tijdelijk onleesbaar te maken voor derden door deze te versleutelen. Verder is een mogelijke maatregel het opstellen van een procedure voor het regelmatig (bijvoorbeeld ieder kwartaal) testen van de doeltreffendheid van de genomen maatregelen ter beveiliging van de verwerking.

Bovendien is VMC ervoor verantwoordelijk dat zowel bij de bepaling van de verwerkingsmiddelen en de ontwikkeling van Vraagmaatje (privacy by design) als bij de

verwerking zelf, maatregelen worden getroffen om de gegevensbescherming te waarborgen. Zo worden risico's verminderd en wordt geld en tijd bespaard. Een voorbeeld hiervan is de beveiliging van de privacykluis die al vanaf de ontwikkeling kan worden bewerkstelligd. Dit principe moet ook worden toegepast op alle applicaties die binnen Vraagmaatje beschikbaar zullen worden gesteld, zoals de persoonlijke mailbox en de anonieme webbrowser. Naast de privacy by design moet worden uitgegaan van standaardinstellingen die zo veel mogelijk ten gunste van een betrokkene moeten zijn, zoals door opt-ins (privacy by default).

De zojuist genoemde anonieme proxyserver is tevens een goede maatregel om de beveiliging voor de rechten van een betrokkene te waarborgen. Doordat de communicatie tussen de gebruiker en een andere computer via een proxy verloopt, wordt het moeilijker gemaakt voor derden om de gegevens van deze gebruiker te achterhalen. Hierdoor worden zijn persoonsgegevens tot op zekere hoogte geanonimiseerd. Verder is het, ongeacht of dit verplicht is, verstandig een onafhankelijke toezichthouder aan te stellen die tevens toetst of de beveiligingsmaatregelen binnen Vraagmaatje optimaal zijn.

Ten slotte is het essentieel dat VMC ervan op de hoogte is dat bij een datalek met een risico voor de rechten van een betrokkene of derde, dit binnen 72 uur dient te worden gemeld bij de Autoriteit Persoonsgegevens (AP). Wanneer deze een hoog risico inhoudt voor de betrokkene of derde, moet ook diegene op de hoogte worden gesteld van deze inbreuk.

Privacy Impact Assessment (PIA) en voorafgaande raadpleging

VMC is verplicht om bij verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten van natuurlijke personen, vóór de verwerking een PIA uit te voeren van het effect van de beoogde verwerkingshandelingen. Deze verwerkingen zullen er zijn, zeker gezien het feit dat in grote mate gebruik wordt gemaakt van nieuwe technologieën, waaronder kunstmatige intelligentie, die een hoog risico met zich mee kunnen brengen. Wanneer uit een PIA blijkt dat de verwerking een hoog risico zou opleveren indien VMC geen (extra) maatregelen neemt om het risico te beperken, is zij verplicht voorafgaand aan de verwerking de AP te raadplegen.

Functionaris voor gegevensbescherming (FG)

VMC is in ieder geval in het begin nog niet verplicht een FG aan te stellen. Pas als zij hoofdzakelijk zou zijn belast met de grootschalige verwerking van bijzondere categorieën gegevens, zou zij hiertoe verplicht zijn. Op dit moment is zij weliswaar voornemens bijzondere persoonsgegevens te verwerken, maar is dit 'slechts' een onderdeel van alle verwerkingen. Desondanks is het voor VMC verstandig om een onafhankelijke toezichthouder op te richten of aan te wijzen die controleert of VMC aan de gegevensbeschermingsregels voldoet en blijft voldoen.

Boetebevoegdheid Autoriteit Persoonsgegevens

Indien VMC zich niet houdt aan de regels uit de AVG, is een betrokkene gerechtigd tot het instellen van beroep bij een rechter, het starten van een civiele procedure of het indienen van een klacht bij de AP. Ook riskeert zij, afhankelijk van de overtreden bepaling, een last onder bestuursdwang of een bestuurlijke boete met een hoogte oplopend tot € 10.000.000,- respectievelijk € 20.000.000,-;

Tot slot: betalen met persoonsgegevens en ethische aspecten

Het is juridisch toegestaan om gebruikers te laten betalen met persoonsgegevens, omdat bij de regels uit de AVG geen onderscheid wordt gemaakt tussen de situatie waarin wel of niet met geld moet worden betaald voor een dienst. Essentieel blijft dat alle relevante regels uit de AVG, met name het transparantiebeginsel en de toestemming, in acht worden genomen. Hierbij moet ervoor worden gezorgd dat er geen twijfel kan bestaan over de uitdrukkelijkheid en ondubbelzinnigheid van deze toestemming. Desondanks valt te betwijfelen of dit in de startfase de juiste keuze is. Praktisch gezien zou eerst moeten worden beoordeeld of het verdienmodel niet te complex wordt. Er zou dan namelijk bekeken moeten worden van welke

gegevens een gebruiker afstand doet tegen welk tarief. Bovendien, als gebruik wordt gemaakt van een dergelijk verdienmodel, zijn wel middelen nodig om voldoende omzet te generen uit deze gegevens. Gezien het voorgestelde verdienmodel lijkt dit in ieder geval voorlopig niet het geval te zijn; er lijkt meer baat te zijn bij direct betalende gebruikers. Bovendien is het een risico wanneer gebruikers de keuze krijgen om weinig persoonsgegevens aan te bieden, omdat Vraagmaatje voor een optimale dienstverlening juist afhankelijk is van deze persoonsgegevens. Tevens is er het risico dat zij het betaalsysteem (te) ingewikkeld vinden. Ten slotte is het met het oog op ethische aspecten de vraag in hoeverre er weerstand zou komen vanuit de doelgroep. Daarvoor is het voor VMC van belang zichzelf te blijven afvragen of een bepaalde handeling moreel gezien wel verstandig is.

In aansluiting op de vorige alinea, verdient het de opmerking dat rekening moet worden gehouden met het feit dat ouderen de primaire doelgroep zijn en zij net als kinderen een kwetsbare groep vormen. Ouderen hebben doorgaans namelijk minder mogelijkheden en vaardigheden om zelf de regie over hun leven te voeren.⁷⁵ Dit is tevens van invloed op veel andere bepalingen uit de AVG, zoals de transparantie waarmee de informatie en communicatie moet verlopen. Dit wordt versterkt door het feit dat het in deze situatie gaat om een digitale dienst en dat ouderen hier doorgaans meer moeite mee hebben dan de gemiddelde persoon. Verder blijkt ook uit de gehouden enquête bij tien ouderen van KBO-Brabant dat transparantie voor hen belangrijk is, met name bij het delen van gegevens met derden.

Mocht het voornemen blijven bestaan om in een later stadium geld te verdienen aan de handel in Big Data in combinatie met algoritmes, moet vooral worden gelet op de eisen die gelden voor pseudonimisering en anonimisering van persoonsgegevens. Een belangrijke kanttekening hierbij is wederom dat deze toevoeging aan het verdienmodel bij gebruikers van Vraagmaatje kan stuiten op weerstand en het vraagstuk van ethisch ondernemen kan oproepen.

§ 5.2 Aanbevelingen

Om bovenstaande conclusies op efficiënte wijze te kunnen implementeren in de werkwijze van VMC, is een checklist en stroomdiagram opgesteld. Door aan deze checklist te voldoen en de stappen uit het stroomschema stapsgewijs te doorlopen, kan worden nagegaan op welk moment de gewenste verwerking voldoet aan de AVG. Aan VMC wordt dan ook geadviseerd de checklist en het stroomdiagram die zijn uitgewerkt op de volgende pagina's te gebruiken.

⁷⁵ Kwetsbare groepen niet altijd zelfredzaam, Eengezondernederland.nl.

Checklist voorafgaand aan aanbieden van Vraagmaatje

Checklist acties voor aanbieden Vraagmaatje

Actie	Gedaan?
1 Kom met de bestuurders van VMC samen om zowel de verantwoordelijkheden als de gewenste verwerkingen en doeleinden en middelen van deze verwerkingen unaniem vast te stellen.	☐
2 Stel termijnen vast voor het wissen van (categorieën) persoonsgegevens of voor een periodieke toetsing van deze gegevens.	☐
3 Stel een gegevensbeschermingsbeleid op met daarin een duidelijke, begrijpelijke uitleg aan de betrokkene over welke persoonsgegevens met welke doeleinden worden verwerkt.	☐
4 Tref maatregelen om betrokkenen hun rechten gemakkelijk uit te laten oefenen.	☐
5 Zorg voor passende beveiliging door passende technische en organisatorische (fysieke) maatregelen te treffen.	☐
5.1 Versleutel, pseudonomiseer of anonimiseer persoonsgegevens waar mogelijk of toegestaan.	☐
5.2 Stel een procedure op voor het testen van de doeltreffendheid van de genomen maatregelen en voer deze procedure regelmatig (ieder kwartaal/halfjaarlijks) uit.	☐
5.3 Neem zowel bij de bepaling van de verwerkingsmiddelen en de ontwikkeling van de software (privacy by design) als bij de verwerking zelf, maatregelen om gegevensbescherming te waarborgen.	☐
5.4 Maak bij de uitvoering van Vraagmaatje gebruik van standaardinstellingen ten gunste van de gebruiker.	☐
6.1 Maak duidelijke afspraken met eventuele verwerkers zoals Capgemini en neem deze afspraken op in een verwerkersovereenkomst.	☐
6.2 Neem in de arbeidsovereenkomst met een eventuele medewerker van VMC een geheimhoudingsclausule op of sluit een afzonderlijke geheimhoudingsovereenkomst met die medewerker.	☐
7 Houd een register met verwerkingsactiviteiten bij.	☐
8 Indien gewenst, stel een onafhankelijke toezichthouder aan, eventueel in de vorm van een functionaris voor gegevensbescherming.	☐
9 Voldoe aan het stroomdiagram op de volgende pagina's.	☐

Legenda



Start/eindpunt



Proces stopt



Paginaverwijzing

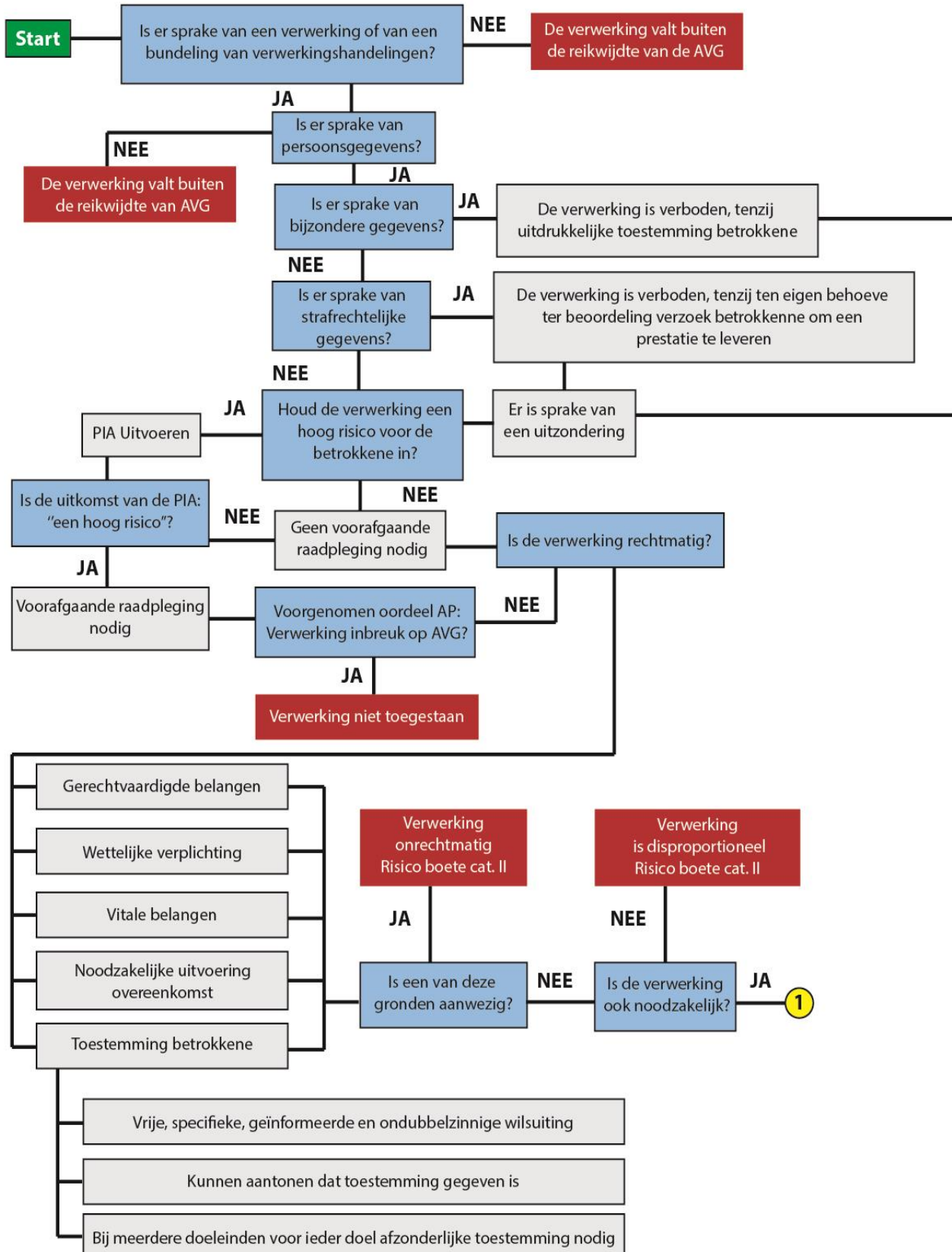


Actie

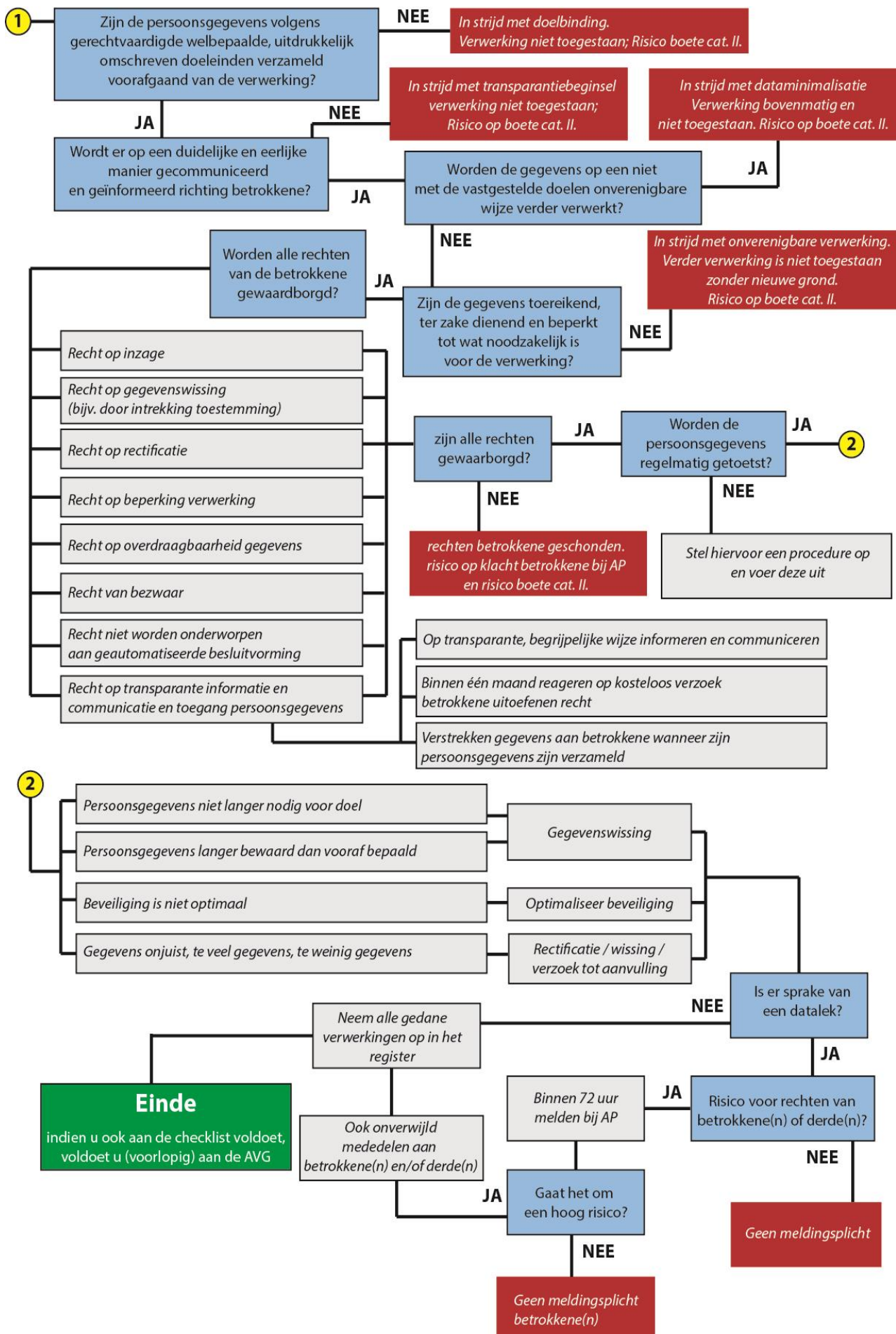


Beslissing/vraag

Stroomdiagram 1/2



Stroomdiagram 2/2



Bronnenlijst

Literatuur

Beelen, van, e.a. 2015

D.C. van Beelen e.a., *Privacy en gegevensbescherming*, Apeldoorn: Maklu Uitgevers 2015.

Fennell, Kroes & Koppejan 2016

S. Fennell, R. Kroes & F. Koppejan, *Privacy wetgeving : inclusief voorgestelde meldplichten, boetes en concept algemene verordening gegevensbescherming*, Oisterwijk: Wolf Legal Publishers 2016.

Holvast 2013

J. Holvast, *De Volkstelling van 1971*, Zutphen: Uitgeverij Paris 2013.

Klous & Wielaard 2016

S. Klous & N. Wielaard, *Wij zijn big data : de toekomst van de informatiesamenleving*, Amsterdam: Uitgeverij Business Contact 2016.

Koekkoek 2000

G. Overkleeft-Verburg, 'Het grondrecht op eerbiediging van de persoonlijke levenssfeer', in: A.K. Koekkoek, *De Grondwet, Een systematisch en artikelsgewijs commentaar*, Deventer: Kluwer 2000.

Kranenborg & Verhey 2011

H.R. Kranenborg, L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Wolters Kluwer Uitgeverij 2011.

Martijn 2016

M. Martijn, *Je hebt wél iets te verbergen : over het levensbelang van privacy*, Amsterdam: De Correspondent 2016.

Wet- en regelgeving en parlementaire stukken

Internetconsultatie, Uitvoeringswet Algemene verordening gegevensbescherming, voorlopige versie d.d. 9 december 2016.

Kamerstukken II 1997/98, 25892, 3, 1-200 (MvT).

Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Privacyrichtlijn)

Verordening (EU) 2016/679 van het Europees Parlement en de Raad, van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming).

Publicaties

Blessing, Historisch Nieuwsblad 2005

M. Blessing, 'Het verzet tegen de Volkstelling van 1971', *Historisch Nieuwsblad* 2005, afl. 8.

Centre for International Governance Innovation & Ipsos 2016

Centre for International Governance Innovation & Ipsos, '2016 CGI-Ipsos Globay Survey on Internet Secutiry and Trust', Waterloo (Canada), 2016.

College bescherming persoonsgegevens 2013

College bescherming persoonsgegevens, 'Onderzoek CBP naar het combineren van persoonsgegevens door Google', Den Haag 2013.

Duhigg, The New York Times 16 februari 2012

C. Duhigg, 'How Companies Learn Your Secrets', *The New York Times Magazine* 16 februari 2012.

Executive Office of the President & President's Council of Advisors on Science and Technology 2014

Executive Office of the President & President's Council of Advisors on Science and Technology, 'Big Data and Privacy: A Technological Perspective', Washington 2014.

Kielman 2010

H.H. Kielman, 'Politiële gegevensverwerking en Privacy: naar een effectieve waarborging' Den Haag 2010.

Maarseveen 2005

J. van Maarseveen, 'Twee eeuwen volkstellingen: de Virtuele Volkstelling 2001 vergeleken met haar voorgangers', *CBS: Sociaal-economische trends* 2005, afl. 1.

Oostrom, Trouw 19 mei 2017

Rianne Oosterom, 'GGZ-instellingen handelden in strijd met de wet door patiëntgegevens te delen. Binnenkort dient een kort geding.', *Trouw* 19 mei 2017.